PENALTY NOTICE

LastPass UK Limited

20 November 2025

[redacted]

CONTENTS

[redacted]

DATA PROTECTION ACT 2018
(PART 6, SECTION 155)
ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER
PENALTY NOTICE

To: LastPass UK Ltd

Of: 5 New Street Square
London
England
EC4A 3TW

FAO: [redacted] (Paul Hastings (Europe) LLP)
[redacted] (LastPass)
Email: [redacted]

20 November 2025

I. INTRODUCTION AND SUMMARY

1. Pursuant to section 155(1)(a) of the Data Protection Act 2018 ("**DPA 2018**"), the Information Commissioner (the "**Commissioner**") by this written notice ("**Penalty Notice**"), requires LastPass UK Ltd ("**LastPass**") to pay the Commissioner a penalty of **£1,228,283**.

2. This Penalty Notice is given in respect of infringements of Article 5(1)(f) UK GDPR and Article 32(1) of the UK General Data Protection Regulation ("**UK GDPR**").

3. This Penalty Notice follows an investigation carried out by the Information Commissioner's Office ("**ICO**") into a personal data breach first reported by LastPass on 30 November 2022. It sets out the Commissioner's conclusions and the reasons why the Commissioner has

[redacted]

decided to impose a penalty, including the circumstances of the infringements and the nature of the personal data involved.

4. In accordance with paragraph 2 of Schedule 16 to the DPA 2018, the Commissioner issued a notice of intent ("**NOI**") to LastPass on 29 May 2025 setting out the reasons why the Commissioner proposed to issue LastPass with a penalty notice. In that NOI, the Commissioner indicated that the amount of the penalty he proposed to impose was £2,696,745.

5. On 9 July 2025, LastPass made written representations (the "**Written Representations**") in response to the NOI.[1] LastPass made oral representations at a hearing on 23 July 2025 (the "**Oral Hearing**"). On 15 August 2025, LastPass provided written responses to questions asked by the Commissioner's staff at the Oral Hearing.[2] In reaching the decision to issue this Penalty Notice, the Commissioner has taken full account of LastPass' representations and, where appropriate, the Penalty Notice makes specific reference to them.

6. The Commissioner finds that, between 31 December 2021 and 31 December 2024 (the "**Relevant Period**"), LastPass infringed Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR (the "**Infringements**"). In summary, LastPass failed to implement appropriate technical and organisational measures to ensure (i) an appropriate level of security for the personal data for which it was responsible; and (ii) the ongoing confidentiality and integrity of its processing systems and services as required by Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR.

7. The Infringements resulted from LastPass allowing its employees, including senior employees with access to highly confidential corporate credentials, to:

   (a) access both their Personal[3] and Employee Business[4] LastPass

[1] Letter from Paul Hastings (Europe) LLP to the ICO, 9 July 2025
[2] Letter from Paul Hastings (Europe) LLP to the ICO, 15 August 2025
[3] As defined in paragraph 31 below.
[4] As defined in paragraph 31 below.

[redacted]

accounts from a personal device, where the latter contained the decryption keys required to access LastPass customers' personal data; and

(b) combine their Personal and Employee Business LastPass accounts so that they could be accessed by a single master password.

8. As a consequence of LastPass' failure to implement and use appropriate technical and organisational measures, contrary to Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR, personal data relating to 1,631,410 UK-based LastPass customers was unlawfully accessed and exfiltrated by a threat actor.[5]

9. The Commissioner finds that the Relevant Period began on 31 December 2021 and ended on 31 December 2024. 31 December 2021 is the date upon which the entity formerly known as LogMeIn, Inc. ("**LogMeIn**") completed a corporate restructuring which resulted in the separation of its password management business (the "**LastPass Business**") and its business communication and software service operations into two distinct subsidiary structures under a common non-operating parent entity known as LMI Parent, L.P.[6] 31 December 2024 is the date upon which LastPass completed the rollout of company-owned mobile devices to all employees pursuant to a policy which prohibits its employees from using corporate devices for personal purposes and using personal devices for business purposes, unless explicitly approved.[7]

10. This Penalty Notice is issued in respect of the Infringements on the basis that, in all the circumstances, and having regard to the matters listed in Articles 83(1) and 83(2) UK GDPR, the Commissioner considers that a

[5] For the purposes of this Penalty Notice, the Commissioner has referred to "the threat actor." However, the Commissioner has not been provided with evidence which confirms that the Incidents were attributable to a single individual or group, meaning that it remains a possibility that multiple different threat actors were involved in the Incidents.
[6] Letter from Paul Hastings (Europe) LLP to the ICO, 18 October 2024 (responding to an Information Notice issued by the Commissioner dated 19 September 2024)
[7] Email from Paul Hastings LLP to the ICO, 6 November 2025

[redacted]

penalty of £1,228,283 adequately reflects the seriousness of the Infringements and is an effective, proportionate and dissuasive response to the Infringements.

II. RELEVANT LEGAL FRAMEWORK

11. Chapter II of the UK GDPR sets out the principles relating to the processing of personal data. Article 5(1)(f) UK GDPR provides that "[p]*ersonal data shall be…processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*"

12. Article 32(1) UK GDPR, which specifically addresses the security of processing, provides that "[t]*aking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

    (a) *the pseudonymisation and encryption of personal data;*

    (b) *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*

    (c) *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and*

    (d) *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."*

13. In addition, Article 32(2) UK GDPR provides that when "*assessing the*

[redacted]

appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

14. Other relevant provisions of the UK GDPR and the DPA 2018 are set out below, where relevant, in the sections dealing with the Infringements.

15. The legal framework for setting administrative penalties is set out below in **Section V: Decision to impose a penalty**.

III. FACTUAL BACKGROUND

16. This section summarises the circumstances of the Infringements that are the subject of this Penalty Notice for the purpose of providing the background to the Commissioner's findings of infringement. It does not purport to set out an exhaustive account of all of the details of the events that have led to the issue of this Penalty Notice.

(a) Corporate Background

17. On 31 December 2021, the entity previously known as LogMeIn announced a corporate restructuring pursuant to which its business communication and IT support software operations (rebranded as "GoTo" on 2 February 2022 and herein referred to as the "**GoTo Business**")[8] and the LastPass Business were separated into two distinct subsidiary structures managed by two separate chief executives and leadership teams, but operating under a common holding entity known as LMI Parent, L.P.[9] The corporate restructuring completed in May 2024.[10]

18. LastPass is a private limited company (company number 13720418) registered in England. It was incorporated on 3 November 2021 and is

[8] Announcing GoTo (2 February 2022) (accessed 6 March 2025)
[9] Letter from Paul Hastings (Europe) LLP to the ICO, 18 October 2024 (responding to an Information Notice issued by the Commissioner dated 19 September 2024)
[10] LastPass Completes Journey to Become an Independent Company with Enhanced Cybersecurity Focus and Executive Leadership Team - LastPass (accessed 6 March 2025)

[redacted]

a wholly-owned subsidiary of LastPass Ireland Limited.[11] LastPass Ireland Limited is a [redacted] subsidiary of [redacted], which is in turn a [redacted] subsidiary of [redacted]. [redacted] is a [redacted] subsidiary of [redacted], which is itself [redacted] owned by LMI Parent, L.P.,[12] a holding company jointly owned by Francisco Partners Management L.P., a private equity firm incorporated as a limited partnership in the [redacted] and headquartered in the US state of California, and Elliott Investment Management L.P., an investment management company incorporated as a limited partnership in the US state of Delaware and headquartered in Florida.[13]

19. On 31 December 2021, as part of the corporate restructuring referred to in paragraph 17 above, LastPass entered into an agreement to purchase the LastPass Business in the UK from GoTo Technologies UK Limited for £4,101,723.[14] On 1 January 2022, 31 employees of GoTo Technologies UK Limited transferred to LastPass as part of this restructuring of the LastPass Business.[15]

20. Following the completion of these agreements, LastPass describes itself as a "*market leading password management and single sign-on solution that gives individuals, business teams and enterprises the ability to securely store, create and access the user identity and log-in credentials for thousands of online applications and websites.*"[16] LastPass offers a subscription-based software service, including both free and fee-based

[11] Letter from Paul Hastings (Europe) LLP to the ICO, 18 October 2024 (responding to an Information Notice issued by the Commissioner dated 19 September 2024)
[12] Letter from Paul Hastings (Europe) LLP to the ICO, 18 October 2024 (responding to an Information Notice issued by the Commissioner dated 19 September 2024)
[13] LastPass Completes Journey to Become an Independent Company with Enhanced Cybersecurity Focus and Executive Leadership Team - LastPass (accessed 6 March 2025)
[14] LastPass UK Limited Reports and Financial Statements for Year Ended 31 December 2023
[15] LastPass UK Limited Reports and Financial Statements for Year Ended 31 December 2023
[16] LastPass UK Limited Reports and Financial Statements for Year Ended 31 December 2023

[redacted]

premium options. LastPass' revenue is principally derived from fees paid by subscribers to its premium service, who range from individuals and small and medium-sized businesses to multi-national enterprises.[17]

21. During the year ended 31 December 2023, LastPass generated revenue in excess of £14.4 million,[18] whilst in the year ending 31 December 2024, LMI Parent, L.P. reported a global annual turnover of $[redacted] (approximately £[redacted])[19], of which $[redacted] (approximately £[redacted]) was generated by the LastPass Business.

22. At the time of the Infringements, LastPass estimated that it had approximately 1.9 million UK users, comprised of approximately 1.6 million personal or family account holders[20] and 300,000 Business or Teams[21] users who had been provided with accounts through their employer.[22] Whilst LastPass acknowledges that it is the controller of the personal data associated with personal or family accounts, it states that it acts as the processor for organisations which use its Business or Teams services, which are themselves the controllers of their employees' personal data which is stored in their company-provided LastPass vaults.[23]

23. LastPass advertises its "*best-in-class encryption*" which it claims protects customers' private data[24] and notifies them when it is

[17] LastPass UK Limited Reports and Financial Statements for Year Ended 31 December 2023
[18] LastPass UK Limited Reports and Financial Statements for Year Ended 31 December 2023
[19] LMI Parent, L.P. consolidated financial statements for the year ended 31 December 2024. In this Notice, the conversion of figures from US Dollars to Pound sterling has been calculated using the average of the GBP/USD exchange rates on the first and last trading days of the period covered by LMI Parent, L.P.'s consolidated financial statements for the year ended 31 December 2023 (2 January 2024 and 31 December 2024)
[20] Family accounts are designed for personal use and allow a designated family member to manage accounts for up to six individual members of their family
[21] Business or Teams accounts are held by companies and other commercial entities which use LastPass' services as a password management solution.
[22] Letter from Paul Hastings (Europe) LLP to the ICO, 13 December 2023
[23] Letter from Paul Hastings (Europe) LLP to the ICO, 12 July 2023
[24] Zero-Knowledge Encryption & Security Model - LastPass (accessed 6 March 2025)

[redacted]

compromised.[25] LastPass currently holds several third-party certifications,[26] including ISO 27701:2019,[27] ISO 27001:2022,[28] SOC2 Type II[29] and BSI C5[30].

(b) Password vaults and *"Zero Knowledge"* encryption

24. LastPass offers a password manager product which provides users with an encrypted password vault in which they can store passwords, login credentials, payment information, addresses and secure notes. In addition, LastPass offers users the ability to autofill online forms, generate secure online usernames and passwords, store payment information in a digital wallet and automatically monitor and detect if their information has been exposed online.[31]

25. LastPass employs local-only encryption, which is designed to allow only the LastPass user to decrypt and access their data. Under this model, all confidential data stored in LastPass users' vaults is encrypted and decrypted exclusively on the user's local machine, and the data is only synced with LastPass servers after it has been encrypted, so LastPass

[25] Dark Web Monitoring & Alerts - LastPass
[26] LastPass Trust Center (accessed 6 March 2025)
[27] The ISO 27701 series is privacy extension to the international information security management standard (ISO 27001) which specifies the requirements for and provides guidance for establishing, implementing, maintaining and continually improving a privacy information management system, whilst also providing a set of privacy-specific requirements, controls and control objectives. - ISO 27701 Privacy Information Management | IT Governance UK
[28] The ISO 270001 series sets out a framework for all organisations to establish, implement, operate, monitor, review, maintain and continually improve an information security management system - What is ISO/IEC 27001? | Implement, Certify & Comply
[29] Service Organisation Control Type 2 is a cybersecurity compliance framework developed by the American Institute of Certified Public Accounts, the primary purpose of which is to ensure that third-party providers store and process client data in a secure manner. The framework specifies criteria to uphold high standards of data security, based on five trust service principles: security, privacy, availability, confidentiality and processing integrity. - SOC 2® - SOC for Service Organizations: Trust Services Criteria | AICPA & CIMA
[30] The C5 Cloud Computing Compliance Criteria Catalogue specifies minimum requirements for secure cloud computing and is primarily intended for professional cloud providers, their auditors and customers. The C5 catalogue was first published in 2016 by the German Federal Office for Information Security (BSI) with the aim of building trust between cloud services providers and their customers. The C5 catalogue was revised in 2019 to take account of the latest developments and increase its quality. - BSI - C5 criteria catalogue
[31] Password Vault Software - LastPass Digital Vault (accessed 6 March 2025)

[redacted]

itself never has access to the unencrypted data. LastPass also does not have access to, nor does it store the plaintext "*master password*" that users must enter in order to access their account. As a result, LastPass is unable to decrypt the data stored in a user's vault. The data within a user's vault is only decrypted locally on their own device after the master password is successfully entered, including when the user accesses their account via the internet or a mobile app.[32] LastPass refers to this protection of the contents of users' vaults as "*zero knowledge*" encryption.[33]

26. LastPass combines its local-only encryption model with one-way salted[34] hashes[35] in order to secure the data stored by its customers in their vaults whilst also allowing for online access and cloud syncing. LastPass encrypts user data with Advanced Encryption Standard ("**AES**") in Cipher Block Chaining ("**CBC**") mode with a 256-bit key generated from each user's master password. This means that, when a user first creates a LastPass account, their master password is converted, via hashing, to an encryption key with the username as the salt. This process is performed entirely on the user's device. At the time of the Incidents a default of 100,100 rounds of PBKDF2-SHA256[36] was used to create the encryption key, although this value was customisable by each user.[37] An additional round of hashing is performed in order to generate the master password authentication hash. The hash is then sent to the

[32] LastPass Technical Whitepaper (accessed 13 October 2025)
[33] Zero-Knowledge Encryption & Security Model - LastPass (accessed 6 March 2025)
[34] "Salting" refers to the practice of adding random data to credentials during the hashing process in order to help protect against some forms of brute force cyber attacks. - Glossary - NCSC.GOV.UK
[35] Cryptographic hash functions, or "hashing," transform input data of any size into fixed-length outputs known as "hash values" or "message digests." Hashing is intended to be one-way, meaning that a person who obtains a list of hash values should not be able to work out what the original input was, even if they know what hash function was used to create the values. - Pseudonymisation | ICO
[36] LastPass uses Password-Based Key Derivation Function (PBKDF2) applying Secure Hash Algorithms-256 (SHA-256) to convert a user's master password into an encryption key.
[37] The current default number of PBKDF2 iterations is 600,000. - LastPass Technical Whitepaper (accessed 13 October 2025)

[redacted]

LastPass server to be used for authentication purposes when the user logs in. The user's master password and the encryption key are never sent to the LastPass servers and LastPass cannot reverse the authentication hash that it receives to derive the user's master password.[38]

(c) LastPass "Personal" and "Business" accounts

27. LastPass markets and sells various services designed for both individual customers (its Free, Premium and Family plans) and businesses (its Business and Teams plans).[39] The Infringements relate to processing conducted by LastPass in connection with the provision of its services to individual customers, not its services to businesses.

28. Individual account holders generally use LastPass for personal use, such as generating and storing passwords for third-party accounts or applications. The service features available to individual account holders vary depending on whether the user subscribes to the Free or Premium[40] version of the service.

29. Family accounts[41] are also intended for personal use and allow a designated "*Family Manager"* to provide and manage individual LastPass accounts for up to six individual members of their family.[42]

30. LastPass "*Business*"[43] and "*Teams*"[44] users are typically employees of companies that have purchased the LastPass product as an enterprise password management solution.[45]

31. Prior to the separation of the LastPass Business from the GoTo Business, all employees of the GoTo Business received a company issued LastPass

[38] LastPass Technical Whitepaper (accessed 13 October 2025)
[39] Letter from Paul Hastings (Europe) LLP to the ICO, 14 September 2023
[40] Premium Password Manager - LastPass (accessed 6 March 2025)
[41] Family Password Manager - LastPass (accessed 6 March 2025)
[42] Letter from Paul Hastings (Europe) LLP to the ICO, 13 December 2023
[43] Business Password Management - LastPass Business (accessed 6 March 2025)
[44] Try a Team Password Manager for Secure Password Sharing - LastPass (accessed 6 March 2025)
[45] Letter from Paul Hastings (Europe) LLP to the ICO, 13 December 2023

account to be used for generating and storing corporate credentials (an "**Employee Business account**"). These Employee Business accounts were provisioned and managed by the GoTo Business' IT team as part of the GoTo LastPass tenant. Employees were also provided with access to a complimentary LastPass Premium account for the storage of their own personal credentials (a "**Personal account**").[46] At the time of the Incidents, it was common practice for LastPass employees to have linked their Employee Business and Personal accounts,[47] with this feature also being promoted to LastPass' business customers from May 2019 onwards.[48] Once the accounts were linked, the same master password could be used to access the data stored in the two separate LastPass accounts, one for personal credentials and the other for business credentials.[49]

32. On 22 May 2023, LastPass amended its policy to prohibit employees to link their Employee Business and Personal accounts.[50]

33. As of the date of this Notice, LastPass continues to allow the administrators of LastPass Business or Teams accounts to recommend or require individual end users (i.e. their employees) to link a personal LastPass account to their company-issued LastPass account. Administrators of LastPass Business and Teams accounts also have the option to prohibit end users from linking a personal LastPass account to their company-issued LastPass account.

(d) Impacted System

34. For data backup and disaster recovery purposes, LastPass' database (including data stored in end-user password vaults) is routinely backed up to Amazon Web Services ("**AWS**") Simple Storage Service ("**S3**")

[46] LastPass' Written Representations, 9 July 2025, paragraph 3.4(a)
[47] LastPass' Written Representations, 9 July 2025, paragraph 3.4(b)
[48] When Work Meets Personal: How LastPass Linked Accounts Work (accessed 25 July 2025)
[49] LastPass' Written Representations, 9 July 2025, paragraph 3.4(c)
[50] LastPass' Written Representations, 9 July 2025, paragraph 3.4(f)

[redacted]

buckets. AWS describes the S3 system as a commonly-used general purpose cloud storage service which allows for the storage and protection of any amount of data for a range of uses, "*such as data lakes, websites, mobile applications, backup and restoration, archiving, enterprise applications, support for Internet of Things devices and big data analytics.*"[51]

35. LastPass uses server-side encryption with a customer-provided key (the "**SSE-C Key**") to secure the AWS S3 buckets that are used for the backup storage of its production databases (the "**Backup Database**"). LastPass manages the encryption and decryption of the SSE-C Key.

36. At the time of the Incidents, LastPass used physical datacentres for its production environment and the AWS S3 buckets were only used for backup storage. LastPass used [redacted], a software configuration management and infrastructure automation tool,[52] to automate the deployment and management of its infrastructure. However, the AWS SSE-C Key itself and other keys and secrets were not embedded within the code stored within the [redacted] control repository. These values were encrypted and managed using a [redacted] module called [redacted].[53]

37. During the Relevant Period, the Backup Database contained data including company names, end-user names, website URLs, billing addresses, email addresses, telephone numbers and IP addresses. This data was encrypted whilst it was stored in the AWS S3 buckets, but was decrypted when accessed and exfiltrated by the threat actor. Data stored within LastPass password vaults, including usernames, passwords and secure notes, was also held on the Backup Database.

---

[51] What is Amazon S3? - Amazon Simple Storage Service (accessed 6 March 2025)

[52] [redacted] uses a control repository to keep each of the environments that it manages similarly updated. This control repository is where the various code, templates and configuration scripts used in connection with [redacted] deployments are stored. Some of these scripts contain "values", which can refer to sensitive data, including keys, credentials and other secrets. - [redacted] (accessed 28 July 2025).

[53] LastPass' Written Representations, 9 July 2025: paragraphs 4.7 – 4.8

[redacted]

However, the data stored within LastPass password vaults remained in an encrypted state at all times as LastPass' "*zero knowledge*" encryption system means that data stored within users' password vaults can only be decrypted by the user's "*master password,"* which is solely managed by the user and is not stored, managed or accessed by LastPass, as further explained at paragraphs 25 and 26 above.[54] The only exception to this were website URLs saved in LastPass password vaults, which were not subject to additional encryption and were therefore visible to both LastPass and the threat actor.[55]

38. In order to access and download the Backup Database held in the S3 buckets, two separately stored credentials were required, specifically the SSE-C Key, which was encrypted and stored within a source code repository,[56] and an access key (the "**AWS Access Key**"). As the SSE-C Key was encrypted at rest, a decryption key was also required in order to decrypt the SSE-C key for use.

39. The decryption key needed to decrypt the SSE-C Key was stored within the Employee Business account vaults of four senior LastPass employees, including the Senior Development Operations engineer who was targeted during Incident 2 (the "**Senior Development Operations Engineer**").[57]

(e) Incident 1

40. On 11 August 2022, an AWS GuardDuty alert[58] was triggered when a LastPass employee's account attempted to manipulate AWS Identity and

[54] Letter from Paul Hastings (Europe) LLP to the ICO, 12 July 2023
[55] Letter from Paul Hastings (Europe) LLP to the ICO, 22 February 2023
[56] A source code repository is a centralised platform where developers store and maintain source code, configuration files and other assets relevant to software projects. Source code repositories facilitate collaboration between developers, allow for changes to be tracked and allow for the restoration of previous versions of source code where necessary
[57] LastPass' Written Representations, 9 July 2025: paragraph 4.9
[58] AWS GuardDuty alerts are generated in response to potential security issues detected within AWS accounts, workloads and data. AWS GuardDuty generates alerts whenever it detects unexpected and potentially malicious activity in an AWS environment. - Understanding and generating Amazon GuardDuty findings - Amazon GuardDuty

[redacted]

Access Management commands[59] which the account in question was not configured to allow ("**Incident 1**"). LastPass' Security Operations Centre ("**SOC**") is responsible for conducting the initial investigation following such alerts. If the SOC cannot verify the activity which triggered the alert as legitimate, it contacts other LastPass teams for assistance, which it did following Incident 1. On 12 August 2022, LastPass initiated a formal investigation in accordance with its Incident Response Plan.[60] On 13 August 2022, LastPass engaged Mandiant, an American cybersecurity firm to assist with the incident response.[61]

41. In the course of the investigation it was determined that the alert was linked to an IP address associated with a corporate MacBook Pro laptop issued to a LastPass software developer [redacted] (the "**Software Developer**").[62] The threat actor compromised the Software Developer's laptop, accessed the LastPass development environment,[63] including technical documentation, such as corporate online forums which described how the LastPass development environment operated, and exfiltrated 14 out of approximately 200 LastPass source code repositories.[64] LastPass later confirmed in a blog posted on its website that its development environment does not contain any customer personal data.[65]

42. Due to anti-forensic activity[66] performed by the threat actor, as well as a scheduled operating system upgrade which coincided with Incident 1, LastPass' investigation was unable to determine the means by which the

[59] Access Management- AWS Identity and Access Management (IAM) - AWS (amazon.com) (accessed 6 March 2025)
[60] Letter from Paul Hastings (Europe) LLP to the ICO, 12 July 2023
[61] Incident 1 – Additional details of the attack (lastpass.com) (accessed 6 March 2025)
[62] Letter from Paul Hastings (Europe) LLP the ICO, 14 September 2023
[63] A development environment is a software application that assists programmers when developing software code by combining capabilities such as software editing, building, testing and packaging.
[64] Incident 1 – Additional details of the attack (lastpass.com) (accessed 28 February 2025)
[65] Incident 1 – Additional details of the attack (accessed 28 February 2025)
[66] In the context of cyber security incidents, anti-forensic activity refers to techniques used by threat actors to try and disguise their attack, including concealing or manipulating system data in order to impede forensic investigations.

[redacted]

laptop was compromised or the full extent of the threat actor's activity during the course of Incident 1. However, LastPass' investigation was able to determine that the threat actor had used third-party VPN services to disguise the origin of their activity and impersonate the Software Developer. The threat actor was able to "tailgate" the Software Developer to gain access to the LastPass development environment by relying upon the engineer's successful authentication with domain credentials and completion of a multi-factor authentication system.[67]

43. LastPass' investigation found that the data affected during Incident 1 included LastPass' technical documentation and source code for various aspects of the services offered by LastPass. The source code included both unencrypted company credentials and encrypted credentials used for production capabilities, including data backup. Therefore, whilst the source code obtained by the threat actor in the course of Incident 1 enabled them to obtain the SSE-C Key, this remained in encrypted form and did not allow the threat actor to gain access to the Backup Database at this stage, as this also required the separately stored AWS Access Key and the decryption key. No customer personal data or encrypted password vaults were accessed during Incident 1.[68]

44. Following Incident 1, LastPass engaged in a series of actions in an attempt to contain and mitigate the threat actor's activity, including decommissioning, destroying and ultimately rebuilding the affected environment over a six-week period. LastPass took possession of the affected employee's corporate laptop in order to conduct forensic analysis, issued him with a new device and replaced his domain credentials. LastPass also created a remediation plan that included identifying which, if any, credentials to rotate.[69] This involved identifying and inventorying any credentials, secrets and passwords believed to

[67] Incident 1 – Additional details of the attack (accessed 28 February 2025)
[68] Letter from Paul Hastings (Europe) LLP to the ICO, 20 March 2023
[69] LastPass' Written Representations, 9 July 2025: paragraph 4.2

[redacted]

have been impacted. The LastPass incident response team prioritised the rotation of any clear text credentials or secrets that may have been available to the threat actor within the affected source code repositories.[70]

45. The fact that the decryption key required to decrypt the SSE-C Key was stored separately, outside of the control repository accessed during Incident 1 and within the Employee Business account vault of only four senior developers (including the Senior Development Engineer targeted during Incident 2), led LastPass to believe that the SSE-C Key remained safely encrypted. After rotating the clear text credentials or secrets that the threat actor may have accessed, LastPass also rotated the AWS Access Keys (which were not stored in the source code repositories) between 16 August and 18 August 2022.[71] On 20 August 2022, however, after the AWS Access Keys had been rotated, in the course of Incident 2 and unbeknownst to LastPass at the time, the threat actor exported the contents of the Senior Development Operations Engineer's Employee Business account vault. It was only later that LastPass realised that the encrypted SSE-C Key taken during Incident 1 was at risk of being decrypted.[72]

(f) Incident 2

46. On 12 August 2022, the desktop personal computer of a separate LastPass employee, a Senior Development Operations Engineer based in the USA,[73] was compromised by a threat actor. The threat actor gained access to the engineer's computer via their account on the "Plex" streaming service ("**Incident 2**"). At the time, the engineer was using a version of the Plex Media Server that was affected by a known high-risk vulnerability and which allowed for third-party remote command

[70] LastPass' Written Representations, 9 July 2025: paragraph 4.4
[71] LastPass' Written Representations, 9 July 2025: paragraph 4.4
[72] LastPass' Written Representations, 9 July 2025: paragraph 4.9
[73] Letter from Paul Hastings (Europe) LLP to the ICO, 14 September 2023

[redacted]

execution.[74] The Commissioner understands that the LastPass engineer's "Plex" account was maintained for personal purposes and was not connected to their work activities.

47. The threat actor exploited the vulnerability in the Plex system to gain remote access and install a form of keylogger malware on the personal computer used by the engineer to access their LastPass Personal and Business accounts, which were linked. Both the Personal and Business accounts were accessible using the same master password.[75]

48. The Senior Development Operations Engineer was one of the four senior LastPass Development Operations engineers who stored the decryption key, required to decrypt the SSE-C Key, within their Employee Business vaults. Later, on 12 August 2022, the threat actor, having captured the engineer's master password via the keylogger malware, used an exfiltrated trusted device cookie to bypass LastPass' MFA system. The threat actor was then able to remotely access the Senior Development Operations Engineer's Employee Business account vault and obtain the AWS Access Key and the decryption key, which, when combined with the SSE-C Key obtained during Incident 1, could be used to access and download the Backup Database.[76]

49. LastPass later determined that on 19, 20 and 22 August 2022, the Senior Development Operations Engineer's Employee Business account was accessed by an unauthorised third party. AWS logs show that the threat actor used the stolen keys to exfiltrate the contents of the Backup Database and the encrypted personal data within LastPass customers' vaults (from S3 Bucket "[redacted]") between 19 August 2022 and 22 September 2022.[77]

50. On 15 and 22 October 2022, AWS GuardDuty alerts recorded

[74] NVD - CVE-2020-5741 (nist.gov) (accessed 6 March 2025)
[75] LastPass' Written Representations, 9 July 2025: paragraph 3.4(c)
[76] Letter from Paul Hastings (Europe) LLP to the ICO, 25 May 2023
[77] LastPass' Written Representations, 9 July 2025: paragraph 2.1(d)

[redacted]

"[redacted]," specifically that "[redacted]." [78] The AWS GuardDuty alert resulted from the threat actor attempting to perform activities which were outside the scope of those normally conducted by the entity in question.

51. When the SOC received the AWS GuardDuty alert on 15 October 2022 and after being unable to independently verify the activity as legitimate, it contacted the "AWS-LastPass" cloud infrastructure e-mail distribution list in accordance with LastPass' standard operating procedures. However, at the time, this distribution list contained the email address of only one LastPass Director of Software Development Engineering, with the remaining addressees being members of the GoTo Business AWS team. Due to miscommunication between the members of the GoTo Business AWS team and the LastPass engineer, there was a period of confusion regarding who was responsible for investigating and responding to the alert.[79] As a result, the LastPass security operations team were not made aware of the AWS GuardDuty alerts until 2 November 2022, some 18 days after the first AWS GuardDuty Alert from Incident 2 was triggered.[80]

52. On 15 December 2022, LastPass received additional information from AWS which confirmed that the threat actor had exfiltrated a copy of the Backup Database which contained customer account information and metadata associated with customer usage of the LastPass service. Specifically, the exfiltrated data included company names, customer names, billing addresses, email addresses, telephone numbers and IP

[78] Letter from Paul Hastings (Europe) LLP to the ICO, 25 May 2023
[79] Letter from Paul Hastings (Europe) LLP to the ICO, 25 May 2023
[80] Letter from Paul Hastings (Europe) LLP to the ICO, 28 April 2023

[redacted]

addresses. However, LastPass informed the Commissioner that, due to its "*zero knowledge architecture*"[81] whereby it does not store the master password required to access users' password vaults, it remained confident that the highly confidential data stored in users' vaults (including usernames, passwords and secure notes) remained confidential and was not accessible by the threat actor in an unencrypted form.[82] The Commissioner has not seen any evidence during the course of his investigation which indicates that personal data stored in LastPass vaults was, in fact, accessed by the threat actor in an unencrypted form.

53. **Annex 2** to this Notice contains a diagram which illustrates the corporate credentials obtained by the threat actor in the course of the Incidents, the areas accessed by the threat actor and from which personal data was exfiltrated, and the other areas of LastPass' systems which were either not accessed by the threat actor, and/ or from which unencrypted data was not exfiltrated.

(g) Reporting and Notification

54. On 25 August 2022, LastPass published a post on its website informing users that "*an unauthorised third party gained access to portions of source code and some proprietary LastPass technical information.*"[83] On 15 September 2022, an update was published, in which LastPass CEO Karim Toubba confirmed that, following an investigation into Incident 1, "*there is no evidence that this incident involved any access to customer data or encrypted password vaults.*"[84]

55. On 30 November 2022, LastPass submitted a personal data breach report to the ICO, in which it stated that on 27 November 2022, it had "*detected unusual activity within a third-party cloud storage service*" and that its investigation team "*concluded, as a result of its technical*

[81] Zero-Knowledge Encryption & Security Model - LastPass (accessed 6 March 2025)
[82] Letter from Paul Hastings (Europe) LLP to the ICO, 16 December 2022
[83] 12-22-2022: Notice of Recent Security Incident (lastpass.com) (accessed 6 March 2025)
[84] 12-22-2022: Notice of Recent Security Incident (lastpass.com) (accessed 6 March 2025)

[redacted]

investigations, that there was at least a possibility that certain of the data accessed by the threat actor could include personal data."[85]

56. LastPass reported to the ICO that, whilst it was continuing to investigate, the categories of personal data potentially affected included basic personal identifiers and identification data. However, LastPass also indicated that "*based on current information and subject to further investigation,* [it did] *not believe a high risk to data subjects is likely to occur. Our customers' passwords remain safely encrypted due to LastPass' Zero Knowledge architecture."*[86]

57. Also on 30 November 2022, LastPass CEO Karim Toubba published a further update to his initial blog post, in which he stated that LastPass had "*determined that an unauthorised party, using information obtained in the August 2022 incident, was able to gain access to certain elements of our customers' information. Our customers' passwords remain safely encrypted due to LastPass' Zero Knowledge architecture."*[87]

58. This was followed by a further update on 22 December 2022, in which Mr Toubba stated that "*the threat actor copied information from a backup that contained basic customer account information and related metadata, including company names, end-user names, billing addresses, email addresses, telephone numbers and the IP addresses from which customers were accessing the LastPass service. The threat actor was also able to copy a backup of customer vault data from the encrypted storage container…that contains both unencrypted data, such as website URLs, as well as fully encrypted sensitive fields, such as usernames, passwords, secure notes and form-filled data. These encrypted fields remain secured with 256-bit AES encryption and can only be decrypted with a unique encryption key derived from each user's*

[85] Initial Personal Data Breach Report submitted by LastPass to the ICO, 30 November 2022
[86] Initial Personal Data Breach Report submitted by LastPass to the ICO, 30 November 2022
[87] 12-22-2022: Notice of Recent Security Incident (lastpass.com) (accessed 6 March 2025)

[redacted]

master password using our Zero Knowledge architecture. As a reminder, the master password is never known to LastPass and is not stored or maintained by LastPass…There is no evidence that any unencrypted credit card data was accessed."[88]

59. The 22 December 2022 update also warned LastPass customers that "[t]*he Threat actor may attempt to use brute force to guess your master password and decrypt the copies of vault data they took. Because of the hashing and encryption methods we use to protect our customers, it would be extremely difficult to brute force guess master passwords for those customer who follow our password best practices."* The update further stated that "*The threat actor may also target customers with phishing attacks, credential stuffing, or other brute force attacks against online accounts associated with your LastPass vault."* Under the heading "*What Should LastPass Customers Do?"*, LastPass included a summary of its default master password settings and best practices before stating that "*If you use the default settings above, it would take millions of years to guess your master password using generally-available password-cracking technology. Your sensitive vault data… remain safely encrypted based on LastPass' Zero Knowledge architecture. There are no recommended actions that you need to take at this time. However, it is important to note that if your master password does not make use of the defaults above, then it would significantly reduce the number of attempts needed to guess it correctly. In this case, as an extra security measure, you should consider minimizing risk by changing passwords of websites you have stored*."[89]

60. On 1 March 2023, Mr Toubba posted a final update, in which he confirmed that LastPass had "*not seen any threat-actor activity since October 26, 2022"* and provided recommendations as to steps users could take to protect their own data or that of their business, whilst also

[88] 12-22-2022: Notice of Security Incident (accessed 11 March 2025)
[89] 12-22-2022: Notice of Security Incident (accessed 11 March 2025)

[redacted]

setting out details of the steps taken by LastPass in the wake of the Incidents.[90]

61. On 1 March 2023, LastPass also published a detailed breakdown of the categories of user data that were affected by the two incidents.[91] Specifically, LastPass confirmed that the information included users' billing addresses, email addresses, end-user names, IP addresses of devices used to access the LastPass service, mobile numbers and unique identifiers for mobile devices used to access the LastPass service. In the case of LastPass "Business" and "Teams" users, company names, employer identification numbers and tax ID numbers were also compromised. LastPass also warned its users that "*the threat actor may attempt to brute force and decrypt the copies of vault data they took. Our Zero Knowledge encryption architecture is designed to protect customers' sensitive information to defend against attempts to brute force encrypted data. The threat actor may also use some of this data to target customers with phishing attacks, credential stuffing, or other social engineering attacks against online accounts associated with their LastPass vault.*"[92]

62. In the 1 March 2023 update, LastPass directed customers to one of two "*Security Bulletins*", with one designed for users of LastPass' personal products and the other for its Business and Teams users. The "*Security Bulletins*" included "*information designed to help* [LastPass'] *customers secure their LastPass account and respond to these security incidents in a way that* [LastPass] *believe meets their own personal needs or their organization's security profile and environment.*"[93] The "*Security*

[90] 03-01-2023: Security Incident Update and Recommended Actions (lastpass.com) (accessed 6 March 2025)
[91] What data was accessed? (lastpass.com) (accessed 6 March 2025)
[92] What data was accessed? (lastpass.com) (accessed 6 March 2025)
[93] 03-01-2023: Security Incident Update and Recommended Actions (accessed 6 March 2025)

[redacted]

Bulletin" for users of LastPass' personal products[94] included a guide on how to review their LastPass account settings, with the intention of ensuing that customers followed best practices recommended by LastPass.

IV. THE COMMISSIONER'S FINDINGS OF INFRINGEMENT

A. Controllership and Jurisdiction

63. The Commissioner finds that, during the Relevant Period, LastPass was the controller[95] of the personal data of its UK users, which was processed for the purpose of delivering its products and services to individual customers in the UK. The Commissioner's findings are based on evidence which indicates that LastPass determined both the means by which the personal data in the Backup Database was processed (for example, what categories of data were collected, how it was stored and the applicable retention periods) and the purposes for which such processing took place (for example, account management, fraud prevention and product development).

64. This is reflected in LastPass' privacy policy, which states that "*LastPass UK Ltd…is the controller for data collected in connection with* [users'] *use of the Services if you live in the UK."*[96] However, LastPass states in its privacy policy,[97] and has reiterated to the Commissioner, that "*companies who purchase LastPass Business or Teams accounts serve as the data controller for any employee personal data processed, while LastPass would serve as the data processor."*[98]

65. This Penalty Notice only applies to LastPass in its role as a controller of the personal data it processes for the purposes of providing its services for personal use to its individual customers in the UK. This Penalty Notice

[94] Security Bulletin: Recommended Actions for Free, Premium, and Families Customers (accessed 3 September 2025)
[95] As defined in Article 4(7) UK GDPR
[96] LastPass Privacy Policy (accessed 6 March 2025)
[97] LastPass Privacy Policy (accessed 6 March 2025)
[98] Letter from Paul Hastings (Europe) LLP to the ICO, 14 September 2023

[redacted]

does not apply to the processing of personal data relating to the employees of LastPass' Business and Teams customers, and such processing did not form part of the Commissioner's investigation.

66. The provisions of the DPA 2018 and the UK GDPR apply to LastPass pursuant to Article 2(1) UK GDPR and Article 3(1) UK GDPR and section 4(2)(a) and section 207(1A) DPA 2018, as it is a controller which, by virtue of its status as a private limited company incorporated in England and Wales, with an office in London,[99] is established in the UK, and which processed, and continues to process personal data, in an automated or structured manner, in the context of its activities within the UK, specifically, the provision of its password storage services to its personal and business customers in the UK.

B. Nature of the personal data affected

67. On 22 February 2023,[100] LastPass provided the Commissioner with details of the categories of data affected during Incident 2, the number of data subjects affected and confirmed the data that had been accessed by the threat actor in an encrypted or unencrypted form. LastPass informed the Commissioner that:

    a) the email addresses of 1,631,410 UK data subjects had been decrypted and exfiltrated;

    b) the IP addresses of devices used by 1,631,410 UK data subjects to access LastPass vaults had been decrypted and exfiltrated;

    c) the names of 159,809 UK data subjects had been decrypted and exfiltrated;

    d) the telephone numbers of 248,407 UK data subjects had been decrypted and exfiltrated;

    e) the physical addresses of 118,103 UK data subjects had been

[99] Companies House: LastPass UK Ltd (accessed 6 March 2025)
[100] Letter from Paul Hastings (Europe) LLP to the ICO, 22 February 2023

[redacted]

decrypted and exfiltrated; and

f) data stored in the LastPass vaults of 1,216,107 UK data subjects (including website usernames, passwords, secure notes and form-filled data) had been exfiltrated, but in an encrypted form.

68. All of the categories of data listed above, with the exception of the data stored in LastPass vaults,[101] relate to individuals and could, either directly or indirectly, be used by the threat actor to identify them. Therefore, such data constitutes personal data within the meaning of Article 4(1) UK GDPR and section 3(2) DPA 2018 in the hands of the threat actor.

69. Since the Incidents, LastPass has repeatedly emphasised, both in its public statements and in its correspondence with the Commissioner, that the most highly confidential personal data in respect of which it acted as a controller (at least in respect of its individual customers), namely the personal data stored in password vaults, was only accessed and exfiltrated by the threat actor in an encrypted form, with the exception of saved website URLs.

70. LastPass informed the Commissioner that it "*provides customers with a save and autofill feature that allows end users to save the website URL, username and password for a given website to their vault to allow for quick and convenient authentication. The end user usernames and passwords for these websites are "zero-knowledge encrypted" – meaning that LastPass never receives them in an unencrypted state … The database which included these website URLs was stored encrypted*

[101] As stated at paragraphs 25 and 26 above, LastPass uses a local-only encryption model with one-way-only salted hashes in order to generate an authentication hash for the user's master password. The encryption and decryption of data stored in LastPass users' vaults takes place exclusively on the user's device. LastPass does not have access to the user's plaintext master password, nor the encryption key, and cannot reverse the encryption process to obtain the user's master password, thus preventing it from accessing the data within the user's vault (with the exception of saved website URLs) in a decrypted form. This system, referred to as "*zero knowledge"* encryption by LastPass also prevented the threat actor accessing the contents of users' vaults in an unencrypted form.

[redacted]

at rest … however, this database was decrypted from storage by the threat actor using a company managed key, so (unlike end user usernames and passwords, which remained encrypted at all times) the URL fields were not encrypted when the database was exfiltrated."[102]

C. The Infringements

71. The Commissioner has considered whether the facts set out above constitute one or more contraventions of the UK's data protection legislation.

72. For the reasons set out below, the Commissioner finds that LastPass infringed Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR as a result of its failure to process its customers' personal data in a manner that ensured an appropriate level of security of that personal data when taking into account the risks presented by LastPass' processing operations, including protecting it against unauthorised or unlawful processing, accidental loss, destruction or damage.

73. Specifically, the Commissioner finds that LastPass failed to implement appropriate technical and organisational measures to ensure an appropriate level of security for the personal data for which it was responsible and the ongoing confidentiality and integrity of its processing systems and services as required by Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR.

74. This resulted from:

    a) LastPass' practice, at the time that the Incidents occurred, of allowing senior employees with access to highly confidential corporate information to access their Employee Business vaults via the internet from their unmanaged personal devices; and

    b) LastPass' practice, at the time that the Incidents occurred, of allowing its employees to link their Personal and Employee Business

[102] Letter from Paul Hastings (Europe) LLP to the ICO, 7 March 2024

[redacted]

accounts so that they could be accessed by a single master password.

(a) Senior LastPass employees' use of personal devices to access Employee Business accounts

75. The Commissioner finds that LastPass infringed Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR as a result of its practice, at the time that the Incidents occurred, of allowing its employees, including senior employees with access to highly confidential corporate information such as the Senior Development Operations Engineer targeted in Incident 2, to access their Employee Business accounts from their personal devices.

76. The technical and organisational security measures which LastPass was required to implement pursuant to Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR were required to take account of the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing. The Commissioner has found that LastPass, as a provider of software designed to be used for the management of usernames, passwords and other confidential information, with significant technical and financial resources at its disposal, could legitimately have been expected to have enforced stringent security processes and procedures across its operations in order to ensure, to the greatest extent possible, the security of its customers' personal data.

77. The ICO's *Data Protection and Working from Home Guidance*[103] states that whilst allowing employees to use their own devices to access company software is a more cost-effective option, it presents some security risks.[104] Previous guidance published by the ICO on this issue under the Data Protection Act 1998,[105] recommended that organisations

[103] Working from home | ICO (this page from the National Archives displays the ICO guidance in place on 1 June 2022)
[104] Bring your own device – what should we consider? | ICO
[105] ICO: Bring your own device (BYOD) guidance (dated 18 December 2014 and last updated on 29 July 2022)

[redacted]

maintain a clear separation between personal data processed on behalf of the controller and that processed for the device owner's own purposes; limit the choice of devices to those which they had assessed as providing an appropriate level of security for the personal data being processed; and provide guidance to users about the risks of downloading untrusted or unverified applications. The current ICO guidance advises organisations to consider the security risks associated with allowing employees to work from home and use their own devices to access company software, including putting in place mitigation methods to avoid data breaches and providing staff with guidance on how to secure their device.[106]

78. When creating its *Guidance on Data Security*, the ICO worked closely with the National Cyber Security Centre ("**NCSC**") in order to develop an approach which controllers and processors could use when assessing the appropriateness of their technical and organisational security measures.[107] The ICO *Security Outcomes* direct controllers to consider the NCSC's *Device Security Guidance,*[108] including its infographic covering *Home working: Managing the cyber risks* which recommends that organisations use mobile device management software to set up devices with a standard configuration, ensure staff understand the risks of using either their own or company-issued devices outside of the office environment and only permit the use of sanctioned products.[109]

79. The NCSC's *Bring Your Own Device Guidance* addresses the use of personal devices to access corporate data through a web-browser, with this being described as the simplest type of bring your own device ("**BYOD**") system in which users authenticate to a Software as a Service

[106] Bring your own device – what should we consider? | ICO
[107] A guide to data security | ICO (this page from the National Archives displays the ICO guidance in place on 1 June 2022)
[108] Device Security Guidance - NCSC.GOV.UK (published 29 June 2021 and reviewed 13 May 2025)
[109] NCSC: Working from Home: Managing the Cyber Risks (this page from the National Archives displays the NCSC guidance in place on 1 March 2022)

[redacted]

("**SaaS**") application via their web browser. The NCSC guidance states that this approach "*gives rise to a wide range of risks. There are no technical controls that you can reliably enforce to prevent data loss, or access from insecure services. Additionally, you cannot get any confidence in the security or configuration of the devices used.*" The NCSC guidance proceeds to warn that "[A] *compromised device could give an attacker relatively easy access to data as it is rendered in the browser, along with the content of the browser cache credentials, and security tokens of accessed services. If choosing this type of access for BYOD, you should focus on ensuring your employees understand the risks, and particularly why the risks exist. Simply focusing on what needs to be done without the why, could lead to users de-valuing the risks.*"[110]

80. The Commissioner also notes that, during the Relevant Period, LastPass was in possession of an ISO 27001:2022 accreditation, Annex A 8.1 of which is consistent with the ICO's *Data Protection and Working from Home Guidance* and requires organisations to create policies which cover the secure configuration and use of user endpoint devices, including a requirement for devices to be registered and safeguarded against malware intrusions.[111]

81. Following the Oral Hearing, LastPass informed the Commissioner that, at the time of the Incidents, LastPass employees were not able to access the internal LastPass network remotely unless they were using a company-provided laptop and the company-issued Cisco AnyConnect Virtual Private Network software, which required the employee to first verify their identity using multi-factor authentication ("**MFA**").[112] LastPass also stated that at the time of the Incidents it had mobile device management ("**MDM**") software in place, with LastPass employees

[110] Action 4 - Deployment approaches - NCSC.GOV.UK (dated 5 October 2021)
[111] ISO 27001:2022 Annex A Control 8.1 - What's New? | ISMS.online (accessed 6 March 2025)
[112] LastPass Written Representations, 9 July 2025: paragraph 3.2(c)

[redacted]

required to register and enrol their devices in Microsoft Mobile Application Management if they wished to receive company emails on the device through the Outlook application. LastPass' MDM software also required enrolment in Microsoft Authenticator for the purposes of MFA and provided company administrators with the ability to remotely wipe company data from employee devices.[113]

82. However, despite these measures, the Commissioner finds that LastPass failed to adhere to the ICO and NCSC guidance referred to in paragraphs 77 - 79 above, as, at the time of the Incidents, it allowed its employees, including senior employees with access to highly confidential corporate credentials, to access their Employee Business accounts using their personal devices. This was despite the fact that, as the NCSC highlight, if an employee's personal device was compromised, this could give an attacker relatively easy access to the information stored within their Employee Business account. LastPass' practice at the time of the Incidents also demonstrates that it was not consistent with the NCSC's Cyber Assessment Framework ("**CAF**") version 3.1,[114] which provides that allowing "[u]*sers* [to] *connect to your essential function's networks using devices that are not corporately managed"* and allowing privileged users, such as the Senior Development Operations Engineer, to "*perform administrative functions,"* such as accessing locations used to store highly confidential corporate credentials, "*from devices that are not corporately managed"* is indicative of a failure to achieve the CAF's standards in respect of device management.

83. It was this failure to impose a strict separation of work and personal activities which the threat actor exploited during Incident 2. The threat actor exploited a known vulnerability in the software of the third-party streaming service "Plex," which was installed on the personal device of a senior LastPass Development Operations engineer who was based in

[113] LastPass' Written Representations, 9 July 2026: paragraph 3.2(a)
[114] NCSC Cyber Assessment Framework v3.1 (dated 11 April 2022), see section B2.b

[redacted]

the USA and was used the used for his personal purposes.[115] This meant that, despite, LastPass implementing the measures set out in paragraph 81 as a means of protecting against unauthorised remote access to the internal LastPass network, the threat actor, using a keylogger installed by exploiting the vulnerability in the third-party Plex streaming service, was able to obtain the engineer's master password. Thus, the threat actor remotely accessed the Senior Development Engineer's Employee Business vault, which contained the AWS Access Key and the decryption key required, alongside the AWS SSE-C Key exfiltrated during Incident 1, to gain access to the Backup Database.[116]

84. Whilst the vulnerability which the threat actor exploited was found in the third-party "Plex" streaming service installed on the Senior Development Operations Engineer's personal device, the Commissioner has found that LastPass remained responsible for allowing the Senior Development Operations Engineer to access their Employee Business vault, which contained highly confidential corporate credentials, from an unmanaged device on which unverified, non-approved and potentially insecure third-party applications were installed.

85. The Commissioner has found that, when taking into account the sensitivity of the information which was stored within the Senior Development Operations Engineer's Employee Business vault, specifically the AWS Access Keys and decryption key required to decrypt the AWS SSE-C Key, LastPass should have restricted access to this vault to company-managed devices on which only verified, approved and secure software and applications were installed.

86. As stated at paragraph 79 above, the NCSC's *Bring Your Own Device Guidance* highlights that where corporate data is accessed through a web-browser using a personal device, this gives rise to a wide range of risks, with there being no technical controls that can reliably prevent

[115] Letter from Paul Hastings (Europe) LLP to the ICO, 14 September 2023
[116] Letter from Paul Hastings (Europe) LLP to the ICO, 22 February 2023

[redacted]

data loss or prevent access from insecure devices. In light of the sensitivity of the credentials stored within the Senior Development Operations Engineer's Employee Business vault, their use in securing the personal data stored in the Backup Database and the potential consequences of a malicious actor gaining access to those credentials, the Commissioner has found that allowing such a system of remote access to Employee Business accounts, especially for senior employees such as the engineer targeted in Incident 2, represented a failure to implement appropriate technical and organisational security measures in order to ensure the security of the personal data stored in the Backup Database.

87. The Commissioner acknowledges that restricting access to Employee Business accounts to company-issued devices only would not have completely eliminated the possibility of the threat actor infiltrating the Senior Development Operations Engineer's device, noting that the Software Developer during Incident 1 was using a company-issued device. The Commissioner nevertheless considers that implementing such a measure would have significantly reduced the risk of an unsecure, compromised third-party application being used as a means of obtaining the password for, and subsequently gaining access to, the Senior Development Operations Engineer's Employee Business account and thus would have enhanced the security of both the AWS Access Keys and decryption key stored within that account, and, by extension, the personal data within the Backup Database.

88. Judged in light of the guidance in force across the Relevant Period, the Commissioner considers that this measure was, in the context of the highly confidential personal data processed by LastPass, the purposes of its processing and the known threats created by allowing access to highly confidential corporate data via a web browser on personal devices, even with safeguards such as MFA, an appropriate technical and organisational security measure that LastPass ought to have

implemented. Even if such a measure was not adopted for all LastPass employees, the Commissioner finds that it would have been appropriate for those, such as the engineer targeted in Incident 2, with access to highly confidential corporate credentials which were used to secure the personal data stored in the Backup Database.

89. The Commissioner notes that, since the Incidents occurred, LastPass has sought to address the risks previously posed by allowing employees to access their Employee Business vaults using personal devices. Specifically, LastPass issued corporate devices and mobile phones to all employees,[117] implemented [redacted][118] [redacted][119] authentication keys for all employees for enhanced MFA,[120] introduced a new Acceptable Use Policy which expressly prohibits employees from conducting any business activities on their personal devices (and vice versa), and engaged the services of [redacted][121] to restrict employees from accessing non-business approved websites and applications on their corporate devices.[122]

90. In light of the above, the Commissioner finds that LastPass' policy, at the time that the Incidents occurred, of allowing employees to access their Employee Business accounts from personal devices, infringed Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR as it represented a failure to implement appropriate technical and organisational measures to ensure the integrity and confidentiality of the personal data

[117] LastPass' Written Representations, 9 July 2025: paragraph 3.2(d)
[118] A [redacted] is a physical security device (usually in the form of a USB device) which can be used for two factor or multi-factor authentication, password-less logins and to protect against phishing attacks. They can be used to securely log into email accounts, online services, apps, devices and physical spaces. - [redacted] (accessed 31 October 2025)
[119] [redacted] is an open standard developed by the [redacted] for user authentication which aims to strengthen the methods used to sign into online services and protect individuals and organisations against cyber criminality by using phishing resistant cryptographic credentials to validate user identities. - [redacted] (accessed 31 October 2025)
[120] Letter from Paul Hastings (Europe) LLP to the ICO, 15 August 2025
[121] [redacted] is a US-based cyber security company which uses cloud-based services to protect enterprise networks and corporate data.
[122] Letter from Paul Hastings (Europe) LLP to the ICO, 15 August 2025

[redacted]

stored in the Backup Database. Had LastPass prohibited its senior employees with access to highly confidential corporate credentials, from accessing their Employee Business vaults using personal devices, this would have significantly reduced, albeit not completely eliminated, the likelihood of the threat actor being able to access the Senior Development Operations Engineer's Employee Business vault and obtain the AWS Access Key and decryption keys required, alongside the AWS SSE-C Key exfiltrated during Incident 1, to access the Backup Database.

(b) Linking of Employee Business and Personal accounts

91. The Commissioner finds that LastPass infringed Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR as a result of its practice, at the time that the Incidents occurred, of allowing its employees, including senior employees with access to highly confidential corporate credentials, to link their Employee Business and Personal accounts so that they could be accessed using the same master password.

92. As a result of this practice, when, during Incident 2, the threat actor installed a keylogger on the Senior Development Operations Engineer's personal device, they were able to capture the engineer's master password and use it, along with stolen trusted device cookies, to gain access to both his Employee Business and Personal accounts, with the former containing the AWS Access Key and decryption keys required, alongside the AWS SSE-C Key exfiltrated during Incident 1, to access the Backup Database.

93. As stated at paragraph 76 above, the technical and organisational security measures which LastPass was required to implement pursuant to Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR had to take account of the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing. In the context

[redacted]

of passwords, the ICO's *Guidance on passwords in online services*[123] states that "*you should ensure that you stay up to date with the current capabilities of attackers who might try to compromise password systems. You should also consider advice from other sources, such as the* [NCSC] *and GetSafeOnline*," and provides a link to the NCSC's *Guidance on password administration for system owners,*[124] which includes the NCSC's *Password manager buyers guide.*[125]

94. Consideration 14 of the NCSC's *Password manager buyers guide* addresses the risk of personal vaults in a corporate setting and explicitly states that "*there needs to be good separation of home and work passwords. Work passwords should not be accessible from the home vault or vice versa."* This was not the case for LastPass at the time of the Incidents, as it allowed the same master password to be used to unlock both Employee Business and Personal accounts.

95. Additionally, the NCSC's *Password manager buyers guide* states that a "*cloud-sync manager,"* such as LastPass, attracts additional risks due to "*the possibility of a remote attacker gaining access to the password manager account."* The guide states that "*multi-factor support should be used on all cloud-sync password managers"* to mitigate this risk. At the time of the Incidents, LastPass used time-based, one-time password ("**TOTP**") MFA to protect access to both Employee Business and Personal accounts. However, the threat actor was able to bypass the MFA system during Incident 2 via the exfiltration of a trusted device cookie.

96. Therefore, whilst LastPass did implement measures in an attempt to mitigate the risk of allowing its employees to link their Employee Business and Personal accounts, specifically, a requirement for employees to enrol their mobile devices into a mobile device

[123] Passwords in online services | ICO (this page from the National Archives displays the ICO guidance in place on 1 June 2022)
[124] Password administration for system owners - NCSC.GOV.UK (dated 19 November 2019)
[125] Password manager buyers guide - NCSC.GOV.UK (dated 19 November 2019)

[redacted]

management product before then enabling MFA, the Commissioner has found that these measures were not sufficient to ensure that the corporate credentials stored by its senior employees, and the personal data which those credentials protected, were afforded an appropriate level of protection.

97. LastPass' practice of allowing and encouraging employees to link their Employee Business and Personal accounts significantly increased the impact of a single password being compromised. When the threat actor installed keylogger malware on the personal device used by the Senior Development Operations Engineer during Incident 2, they captured the master password which granted access to both the engineer's Employee Business and Personal accounts, thus providing the threat actor with access to the passwords and other confidential credentials, including the decryption keys stored within the engineer's Employee Business vault.

98. In light of the above and taking into account the guidance in force at the time, including that issued by the NCSC, the Commissioner finds that enforcing strict separation of employees' personal and corporate credentials, particularly for senior employees with access to highly confidential corporate data, was an appropriate technical and organisational measure that LastPass ought to have implemented.

99. Whilst the Commissioner acknowledges that prohibiting the linking of Employee Business and Personal accounts would not have definitively prevented Incident 2 from occurring in and of itself, it was an appropriate measure which LastPass should have implemented as part of the steps taken in enhance the integrity and confidentiality of its customers' personal data. If the Senior Development Operations Engineer's accounts had not been linked, the threat actor would have had to remain undetected until the engineer directly accessed his Employee Business account in order to obtain the relevant master password using the keylogger malware installed on his device. This would have created a further layer of protection for the corporate

credentials stored in the engineer's Employee Business account and, by extension, the personal data stored in the Backup Database.

100. Therefore, the Commissioner has concluded that LastPass' practice of allowing its employees, including senior employees with access to the confidential corporate credentials used to secure its customers' personal data, to link their Employee Business and Personal accounts represented a failure to implement appropriate technical and organisational measures to ensure the integrity and confidentiality of its processing systems and services, contrary to Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR.

101. The Commissioner notes that, on 22 May 2023, LastPass began enforcing a policy which prohibits its employees from linking their Employee Business and Personal accounts,[126] whilst its updated Acceptable Use Policy expressly prohibits employees from conducting any business activity on their personal devices (and vice versa).[127]

V. DECISION TO IMPOSE A PENALTY

102. For the reasons set out below, the Commissioner has decided to impose a penalty of **£1,228,283** on LastPass in respect of the Infringements of Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR in accordance with section 155(1)(a) DPA 2018.

A. Legal framework – penalty notices

103. Section 155(1)(a) DPA 2018 materially provides that, if the Commissioner is satisfied that a person has failed to comply with any of the provisions of the UK GDPR specified in section 149(2) DPA 2018, he may, by written notice, require that person to pay to the Commissioner an amount in sterling specified in the notice.

104. When deciding whether to issue a penalty notice to a person, and when

[126] LastPass' Written Representations, 9 July 2025: paragraph 3.4(f)
[127] Letter from Paul Hastings (Europe) LLP to the ICO, 15 August 2025

[redacted]

determining the appropriate amount of the penalty, section 155(2)(a) DPA 2018 requires the Commissioner to have regard to the matters listed in Article 83(1) and (2) UK GDPR, in so far as they are relevant in the circumstances of the case.

105. Article 83(1) UK GDPR requires any penalty imposed by the Commissioner to be effective, proportionate and dissuasive in each individual case.

106. Article 83(2) UK GDPR requires the Commissioner to have due regard to the following factors when determining whether to issue a penalty notice and the appropriate amount of any such penalty in each individual case:

(a) *the nature, gravity and duration of the infringement, taking into account the nature, scope, context and purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered by them;*

(b) *the intentional or negligent character of the infringement;*

(c) *any action taken by the controller or processor to mitigate the damage suffered by data subjects;*

(d) *the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*

(e) *any relevant previous infringements by the controller or processor;*

(f) *the degree of cooperation with the Commissioner in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*

(g) *the categories of personal data affected by the infringement;*

(h) *the manner in which the infringement became known to the Commissioner, in particular whether, and if so, to what extent, the controller or processor notified the infringement;*

[redacted]

(i) *where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;*

(j) *adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and*

(k) *any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement."*

B. The Commissioner's decision on whether to impose a penalty

107. Paragraphs 109 to 188 below set out the Commissioner's assessment of whether it is appropriate to issue a penalty in relation to the Infringements set out in Section IV above. This assessment involves consideration of the factors in Article 83(1) and (2) UK GDPR. The order in which these considerations are set out below follows the ICO's *Data Protection Fining Guidance*, dated March 2024 (the "**Fining Guidance**")[128]:

a) Seriousness of the infringement (Article 83(2)(a), (b) and (g) UK GDPR);

b) Relevant aggravating or mitigating factors (Article 83(2)(c)-(f), (h)-(k) UK GDPR); and

c) Effectiveness, proportionality and dissuasiveness (Article 83(1) UK GDPR).

108. The Commissioner's decision is to impose a penalty.

Seriousness of the Infringements: Article 83(2)(a) UK GDPR

(a) The nature, gravity and duration of the Infringements

109. In assessing the seriousness of the Infringements, the Commissioner has given due regard to their nature, gravity and duration.

[128] Data Protection Fining Guidance | ICO

[redacted]

i. Nature of the Infringements

110. The Commissioner has made a finding of infringement of Article 5(1)(f) UK GDPR, which sets out the integrity and confidentiality principle for the processing of personal data. As stated at paragraph 192 below, an infringement of this provision is subject to the higher maximum statutory penalty,[129] which is indicative of its seriousness.

111. The Commissioner considers that the Infringements constituted a significant contravention of the UK GDPR. As a leading provider of password manager services, LastPass' customers had the right to expect that LastPass would rigorously adhere to its security obligations under the UK GDPR and the industry accreditations it prominently publicised on its website. This is particularly due to the confidentiality of the personal data which customers place within their LastPass vaults, including usernames, passwords and secure notes, which may be used to access a range of accounts and services across other websites and applications.

112. The Commissioner finds that there were technical and organisational measures which LastPass could reasonably have been expected to have implemented at the time of Incidents which would have significantly reduced the risk of a threat actor gaining access to the Backup Database.

113. Incident 2 occurred as a result of the threat actor gaining remote access to a LastPass engineer's personal device through the exploitation of a vulnerability in a third-party application. At the time of the Incidents, LastPass permitted its employees, including those with access to highly confidential corporate data, to access their Employee Business accounts using personal devices on which unverified, potentially insecure and vulnerable third-party applications could be installed. In addition, LastPass also encouraged its employees to link their Employee Business

[129] Article 83(5)(a) UK GDPR

[redacted]

and Personal accounts so that they could be accessed by a single master password.

114. The Commissioner has found that these practices constituted a failure by LastPass to implement appropriate technical and organisational security measures to ensure the integrity and confidentiality of its customers' personal data that was stored within the Backup Database and materially contributed to the threat actor gaining access to the Backup Database.

ii. Gravity of the Infringements

115. When assessing the gravity of the Infringements, the Commissioner has considered the nature, scope and purposes of LastPass' processing, as well as the number of data subjects affected and the level of any damage or distress they have suffered.[130]

116. As regards the **nature** of LastPass' processing, it is of particular significance that LastPass' customers entrust their confidential personal data, specifically the usernames, passwords and secure notes relating to their online accounts, to LastPass for the purpose of increasing the security of their personal data in the online environment. It follows that when devising and implementing its technical and organisational security measures, LastPass should have given particular consideration to:

a) the confidential nature of the personal data it processed;

b) the reasonable expectations of LastPass customers regarding the security measures in place to protect their personal data;

c) the significant risk of LastPass being targeted by cyber-attacks due to the potential value of the personal data it processed to maliciously-motivated threat actors; and

d) the seriousness of the potential consequences of a personal data

[130] Fining Guidance, paragraph 58

[redacted]

breach affecting its systems, including the potential for this to result in its customers' other online accounts being compromised.

117. As regards the **purposes** of the processing, paragraph 59 of the *Fining Guidance*[131] states that the Commissioner may give greater weight to this factor if the relevant processing is central to a controller or processor's main business and commercial activities.

118. The Commissioner considers that the purpose of LastPass' processing is a relevant factor which contributes to the seriousness of the Infringements. LastPass' business model is predicated upon processing personal data supplied by its customers, including confidential personal data such as online account credentials, for the purpose of providing services designed to enhance its customers' online security, and its customers are likely to have specifically selected LastPass' services for this reason.

119. The Commissioner finds that LastPass' processing of personal data for such purposes meant that it was required, pursuant to Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR, to implement particularly robust technical and organisational measures to ensure the integrity and confidentiality of its customers' personal data. However, the Commissioner finds that the technical and organisational measures in place throughout the Relevant Period, specifically its policies regarding the use of personal devices to access Employee Business accounts containing confidential corporate credentials and the linking of Employee Business and Personal accounts, fell below this standard and therefore could not be considered "appropriate" for the purposes of Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR.

120. When considering the **scope** of the processing, the Commissioner has assessed both the territorial scope and the extent and scale of LastPass'

[131] Seriousness of the infringement | ICO

[redacted]

processing.[132]

121. The Commissioner finds that LastPass is the controller[133] directly responsible for the personal data of its approximately 1.6 million Personal or Family account customers in the UK. As stated at paragraph 66 above, the UK GDPR applies to LastPass pursuant to Article 3(1) UK GDPR and section 207(1A) DPA 2018, as it is a controller established in the UK which processed, and continues to process, personal data in the context of its activities within the UK.

122. Paragraph 59 of the *Fining Guidance* states that the greater the **number of data subjects affected** by the infringement, the more weight the Commissioner will give to this factor.[134] In making this assessment, the Commissioner takes into account both the number of data subjects potentially affected, as well as those actually affected, by an infringement.

123. In this case, at the time of the Incidents, LastPass estimated that it had approximately 1.9 million UK customers, 1.6 million of whom held either Personal or Family accounts and in relation to whose personal data LastPass acted as the controller.[135]

124. The number of data subjects whose personal data was actually affected as a result of the Infringements varied according to the type of personal data accessed by the threat actor. LastPass informed the Commissioner that a total of 1,631,410 UK data subjects were affected by the Incidents, with the threat actor having accessed and exfiltrated, in a decrypted format:

    a) email addresses and device IP addresses relating to 1,631,410 UK

[132] Fining Guidance, paragraph 59
[133] As defined in Article 4(7) UK GDPR as the "*natural or legal person, public authority, agency or other body which alone, or jointly with others, determines the purposes and means of the processing of personal data.*"
[134] Seriousness of the infringement | ICO
[135] Letter from Paul Hastings (Europe) LLP to the ICO, 28 April 2023

[redacted]

data subjects;

b) the names of 159,809 UK data subjects;

c) the telephone numbers of 248,407 UK data subjects; and

d) the physical addresses of 118,103 UK data subjects.[136]

125. The threat actor also accessed and exfiltrated the data stored in the LastPass vaults of 1,216,107 UK data subjects, including website usernames, passwords, secure notes and form-filled data, but this remained encrypted at all times as a result of LastPass' *"zero knowledge"* encryption system.[137] As this information was not accessible to the threat actor in a usable format, the Commissioner did not take its exfiltration into account when assessing the seriousness of the Infringements.

126. Paragraph 59 of the Fining Guidance states that when considering the number of data subjects affected by an infringement, the Commissioner may also have regard to the number of complaints received from data subjects about the conduct that has led to the findings of infringement. However, the absence of such complaints will not be regarded as an indication that conduct found to infringe the UK GDPR or DPA 2018 is less serious.[138]

127. LastPass informed the Commissioner that in the months following the public announcement of Incident 2 on 30 November 2022, the company's customer care team recorded an increase in the number of UK users seeking to cancel their subscription and citing the Incidents as their reason for doing so. According to LastPass, between 30 November 2022 and 13 December 2023, 150 UK customers contacted LastPass requesting the cancellation of their accounts and specifically cited concerns raised by the Incidents as their reason for doing so. Of this

[136] Letter from Paul Hastings (Europe) LLP to the ICO, 22 February 2023
[137] Letter from Paul Hastings (Europe) LLP to the ICO, 22 February 2023
[138] Seriousness of the infringement | ICO

[redacted]

cohort of customers, two submitted written demands seeking refunds of the subscription fees they had paid and compensation for the time they had spent changing their online credentials. Whilst one of these complaints was not pursued further, [redacted][139] In addition to the complaints submitted to LastPass, two data subjects complained to the Commissioner about the Incidents.

128. In addition to the cancellation requests, between the public announcement of Incident 2 on 30 November 2022 and 13 December 2023, LastPass observed an increase in the number of UK customers deleting their accounts, with approximately 37,500 doing so.[140] The Commissioner considers that, given their temporal proximity, it is likely that a significant proportion of the additional customer cancellations were related to the Incidents.

129. In assessing the **level of damage suffered**, the Commissioner has had regard to both the actual damage suffered and the potential damage and distress which could have resulted from the Infringements. In particular, the Commissioner has considered the extent to which the Infringements affected the rights and freedoms of LastPass customers in the UK, or otherwise led to them suffering, or being likely to suffer, harm in the form of physical, material or non-material damage.[141]

130. The Commissioner finds that the increased level of cancellation requests submitted by LastPass customers in the UK in the aftermath of the Incidents, particularly the 150 who explicitly cited the Incidents as the reason for their cancellation request, constitutes evidence of the distress or anxiety that data subjects are likely to have experienced as a result of the loss of control over, and associated unauthorised access to, their personal data.

[139] Letter from Paul Hastings (Europe) LLP to the ICO, 13 December 2023
[140] Letter from Paul Hastings (Europe) LLP to the ICO, 13 December 2023
[141] Seriousness of the infringement | ICO

[redacted]

131. The Commissioner acknowledges LastPass' submission that, in its view, the most highly confidential categories of personal data it processes, namely that which is held within customers' vaults, were not available for use by the threat actor after its exfiltration as it remained in an encrypted state. However, despite LastPass using industry-standard encryption algorithms to encrypt the contents of password vaults, the personal data that the threat actor was able to access and exfiltrate from the Backup Database in a decrypted form included identifiers, such as names, email addresses and physical addresses. This could have resulted, and may yet still result, in harm to data subjects, including, but not limited to, brute force and credential stuffing attacks by either the threat actor, or any other person to whom the exfiltrated personal data was disclosed or to whom it may be disclosed in the future.

132. Furthermore, the exfiltration of such personal data also exposed LastPass customers to potential phishing attacks from malicious actors impersonating the operators of the website URLs which were stored in customers' vaults and were obtained by the threat actor in an unencrypted form in the course of Incident 2. The possibility of the Incidents resulting in LastPass customers being targeted by brute force, phishing and/ or credential-stuffing attacks was explicitly acknowledged by LastPass in the detailed breakdown of the categories of data affected during Incident 2 which it published on 1 March 2023.[142]

iii. Duration of the Infringements

133. As stated at paragraph 59 of the *Fining Guidance*, the longer the duration of an infringement, the greater the weight the Commissioner is likely to attribute to this factor due to the greater potential for harm to have occurred.

134. As stated at paragraph 6 above, the Commissioner finds that the Infringements began on 31 December 2021, when the decision to

[142] What data was accessed? (lastpass.com) (accessed 6 March 2025)

[redacted]

separate the GoTo Business from the LastPass Business was announced and continued until 31 December 2024 when LastPass completed the rollout of company-owned mobile devices to all employees pursuant to a policy which prohibits its employees from using corporate devices for personal purposes and using personal devices for business purposes, unless explicitly approved.[143]

(b) The intentional or negligent character of the Infringements (Article 83(2)(b) UK GDPR)

135. The Commissioner finds that the Infringements were negligent, rather than intentional, in nature because LastPass unintentionally breached the duty of care it owed to its customers under the UK GDPR and DPA 2018.[144] Pursuant to Article 24(1) and (2) UK GDPR, controllers are responsible for implementing appropriate technical and organisational measures to ensure and allow them to demonstrate that processing is performed in accordance with the UK GDPR, including the implementation of appropriate data protection processes and policies. It follows that LastPass is responsible for ensuring that its customers' personal data is processed in a manner that ensures an appropriate level of security, including protection against unauthorised or unlawful processing (Article 5(1)(f) UK GDPR) and through the use of appropriate technical and organisational security measures (Article 32(1) UK GDPR).

136. Negligent infringements can be serious and the *Fining Guidance* indicates that the Commissioner may decide to issue a penalty notice in cases where a controller or processor is found to have acted negligently.[145]

137. The Commissioner takes into account all the relevant evidence when considering whether the controller or processor negligently breached the duty of care it owed to data subjects. This requires consideration of the

[143] Email from Paul Hastings LLP to the ICO, 6 November 2025
[144] Fining Guidance, Paragraph 66
[145] Fining Guidance, Paragraph 63

[redacted]

individual circumstances of each case in order to establish the controller or processor's liability[146]

138. When reaching his decision that LastPass negligently breached the duty of care that it owed to its customers, the Commissioner has taken into account all of the relevant evidence, including, in particular:

a) the nature of the service LastPass offers, namely secure password creation and credential storage;

b) the sensitivity of the personal data it processes;

c) the reasonable expectations of LastPass customers regarding the measures in place to protect their personal data, particularly in light of the fact that they are likely to have chosen to use LastPass' services for the purpose of enhancing their digital security;

d) LastPass' practice, at the time of the Incidents, of allowing senior employees with access to confidential corporate credentials, to access their Employee Business accounts using personal devices, the security of which LastPass could not ensure;

e) LastPass' practice, at the time of the Incidents, of encouraging its employees, including those with access to confidential corporate credentials, to link their Employee Business and Personal accounts so that they could be accessed using a single master password; and

f) the financial and technical resources available to LastPass.

139. In light of the factors set out in paragraph 138 above, the Commissioner finds that LastPass could reasonably have been expected to have implemented more rigorous technical and organisational measures to prevent unauthorised access to its customers' personal data and minimise the risk of its integrity and confidentiality being compromised.

140. The Commissioner considers that, particularly in the context of the

[146] Fining Guidance, Paragraph 67

[redacted]

increase in remote working during and after the Covid-19 pandemic, LastPass should have reviewed and updated its policies regarding the use of personal devices to access Employee Business accounts, particularly for senior employees. This should have included either a general prohibition on employees using personal devices to access their Employee Business accounts (the position which LastPass subsequently adopted on 22 May 2023) or a risk-based approach to the use of personal devices which ensured that senior employees with access to confidential corporate credentials, including those used to secure the Backup Database, only accessed their Employee Business accounts using company-issued devices on which only verified and security-assessed applications were installed.

141. Furthermore, the Commissioner finds that, due to the nature of its business and the personal data it processes, LastPass should have been especially vigilant to anticipate and detect any threats to the security of its systems and should have implemented all appropriate and technically feasible technical and organisational security measures. It follows that LastPass ought reasonably to have prohibited its employees, or at least those with access to confidential corporate credentials used to secure the Backup Database, from linking their Employee Business and Personal accounts. Whilst doing so would not necessarily have prevented Incident 2 from occurring, it would have meant that the threat actor was required to specifically obtain the password for the Senior Development Operations Engineer's Employee Business account, rather than the master password which gave access to his linked accounts, thus creating a further layer of protection for the decryption keys stored within the engineer's Employee Business vault.

(a) Categories of personal data affected (Article 83(2)(g) UK GDPR)

142. The personal data affected in the course of the Infringement is described above in paragraph 67, and included email addresses, IP addresses, physical addresses, names and telephone numbers.

143. LastPass has repeatedly emphasised to the Commissioner that the usernames, passwords and secure notes stored by users within their LastPass vaults were not accessed or exfiltrated by the threat actor in a decrypted state during the Incidents. Such information is protected by LastPass' "*zero-knowledge"* system, pursuant to which users' vaults are protected by a master password which is never shared with or stored by LastPass. Without access to the master password, the threat actor would have been unable to access the personal data stored in LastPass users' vaults in an unencrypted form.

144. The Commissioner acknowledges LastPass' submission that, in its view, the most confidential categories of personal data relating to its customers that it processes, namely that which is held within customers' vaults, were not available for use by the threat actor after its exfiltration as it remained in an encrypted state and recognises that this prevented the Infringements being of a far greater degree of seriousness. However, the decrypted information that was accessed and exfiltrated by the threat actor included personal data, which could have been used, as further explained at paragraphs 129 to 132 above, and may still be used, in a manner which could result in damage or distress being caused to LastPass customers in the UK.

Conclusion on the seriousness of the Infringements

145. In reaching his decision regarding the seriousness of the Infringements, the Commissioner has considered the nature, gravity and duration of the Infringements, as well as their negligent nature and the categories of personal data affected. The Commissioner has had particular regard to:

a) the extent of LastPass' failure to implement appropriate technical and organisational security measures, particularly:

i. LastPass' practice, at the time of the Incidents, of allowing employees with access to the confidential corporate

credentials used to secure its customers' personal data to access their Employee Business accounts on personal devices on which unverified and potentially vulnerable third-party applications could be installed; and

ii. LastPass' practice, prior to 22 May 2023, of encouraging its employees to link their Employee Business and Personal accounts so that they could be accessed by a single master password, regardless of the confidentiality of the information stored within those accounts;

b) the nature and purpose of the processing performed by LastPass;

c) the evidence of distress experienced by LastPass customers as a result of the unauthorised access to their personal data and the potential for the Infringements to result in LastPass customers being targeted by brute force and phishing attacks; and

d) the negligent nature of the Infringements, specifically the breach of the duty of care owed by LastPass to its customers in respect of maintaining the confidentiality and integrity of the personal data they entrusted to LastPass.

146. The Commissioner has balanced the factors set out at paragraph 145 above, against:

a) the fact that whilst the threat actor was able to access and exfiltrate a significant amount of personal data relating to LastPass customers in a decrypted form, the personal data stored in customers' password vaults remained encrypted at all times due to the effectiveness of LastPass' "*zero knowledge"* encryption system pursuant to which the master passwords required to access customer vaults were never known to, nor stored by, LastPass;

b) the wider technical and organisational security measures, in addition to the "*zero knowledge"* encryption system, that LastPass

had in place at the time of the Incidents;

c) the sophisticated and highly targeted nature of the threat actor, and the speed with which they acted; and

d) the absence of evidence of realised material harm to LastPass customers resulting from the Infringements.

147. In light of the considerations set out above, the Commissioner has concluded that, on balance, the Infringements are of a **low** degree of seriousness.

Relevant aggravating or mitigating factors

(a) Any action taken by the controller or processor to mitigate the damage suffered by the data subjects (Article 83(2)(c) UK GDPR)

148. Paragraph 77 of the *Fining Guidance* states: "*The Commissioner is more likely to take into account measures implemented prior to the controller or processor becoming aware of the Commissioner's investigation as a mitigating factor. Measures that are only implemented after the start of the Commissioner's investigation are less likely to be regarded as a mitigating factor."* The Commissioner informed LastPass of his investigation on 2 December 2022.[147]

149. After the SOC received the AWS GuardDuty alert relating to Incident 1 on 11 August 2022 and was unable to independently verify that the activity was legitimate, it requested further assistance using three email distribution lists, with a formal investigation being launched on 12 August 2022, in accordance with LastPass' Incident Response Plan.[148]

150. In the course of its response to Incident 1, LastPass decommissioned and then destroyed the affected environment before rebuilding it over a six-week period. This involved LastPass deploying a new [redacted],[149]

[147] Email from ICO Casework to Paul Hastings (Europe) LLP, 2 December 2022 (14:33)
[148] Letter from Paul Hastings (Europe) LLP to the ICO, 12 July 2023
[149] [redacted] is a central repository for all data generated by [redacted] or collected from an

[redacted]

creating new credentials and establishing new [redacted] keys.[150] LastPass then systematically migrated all of its existing managed hosts to the new [redacted] server. This process involved LastPass decrypting the existing credentials and [redacted] within the [redacted] module and re-encrypting all of those [redacted] with a new [redacted] key. It was at this point that LastPass rotated the AWS SSE-C Key used to encrypt and decrypt data stored within its S3 buckets despite initially believing that it had not been compromised as the associated decryption keys were stored outside of the affected source code repository in the Employee Business account vaults of four senior LastPass employees, including the Senior Development Operations Engineer targeted in Incident 2. In parallel, in an attempt to further secure its environment, LastPass also rotated the credentials, certificates and secrets which were known to have been obtained by the threat actor, as well as the AWS Access Keys.[151]

151. LastPass also took possession of the Software Developer's MacBook Pro laptop, performed forensic analysis, replaced the device and deleted all existing domain credentials. LastPass' security team also worked with the Software Developer to strengthen their personal security measures.[152]

152. Following Incident 2, LastPass published a blog post alerting users to the Incidents, which it updated as further information became available

organisation's infrastructure and allows for other applications to query and access the data collected and stored by [redacted]. The stored data can be used for monitoring infrastructure health, analysing changes over time and understanding the overall state of an organisation's systems. - [redacted] (accessed 7 October 2025)

[150] [redacted] (accessed 7 October 2025)

[151] Letter from Paul Hastings (Europe) LLP to the ICO, 15 August 2025

[152] Letter from Paul Hastings (Europe) LLP to the ICO, 20 March 2023

during the course of its investigation.[153] The blog included details of measures taken by LastPass to terminate the threat actor's access to its systems, the measures LastPass had implemented, or intended to implement, to secure it systems, and recommended actions which LastPass users could take to protect their own accounts.

153. The Commissioner finds that the measures LastPass implemented in the aftermath of the Incidents successfully terminated the threat actor's access to the Backup Database, but had only a limited effect on mitigating the direct impact of the Infringements on affected data subjects and therefore should be considered a neutral, rather than a mitigating factor in this case.

154. The Commissioner notes that since the Incidents occurred LastPass has implemented a range of strengthened security measures and brought its processing into compliance with Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR. These measures include:

a) the extensive rotation of credentials used by or accessible to the employee whose personal computer was compromised;

b) the deployment of deception technology which augmented existing security programmes;

c) the implementation of an additional cloud security platform with integrations into AWS;

d) the revision of LastPass' MFA access policy to require utilisation of Microsoft Authenticator[154] and the subsequent roll out of a mandatory "*number matching*" enhancement for Microsoft Authenticator ahead of the Microsoft-enforced roll-out in early

[153] 03-01-2023: Security Incident Update and Recommended Actions (lastpass.com) (accessed 6 March 2025)

[154] Microsoft Authenticator is a free app which enables users to sign into a number of accounts without using a password and instead utilising either a pin, facial recognition or a fingerprint for the purposes of user authentication. - About Microsoft Authenticator - Microsoft Support (accessed 7 March 2025)

[redacted]

2023; and

e) enhanced network logging and alerting features.[155]

155. Following the Oral Hearing, LastPass also informed the Commissioner of a series of new security tools, technology and infrastructure measures it had implemented, including:

a) new company-issued and managed iPhones for all employees;

b) [redacted] authentication keys for all employees for enhanced MFA;

c) engaging [redacted][156] for endpoint protection, [redacted][157] for privileged access management, and [redacted] for web filtering of end-user devices and the provision of a secure private access solution for access to LastPass backend systems;

d) endpoint vulnerability management through [redacted][158] to track secure configuration baselines and apply secure configuration;

e) the deployment of a secrets scanning tool, [redacted],[159] to scan code repositories to help identify embedded secrets,[160] passwords and other potentially confidential credentials;

f) subscriptions to third-party threat intelligence platforms,

---

[155] Letter from Paul Hastings (Europe) LLP to the ICO, 16 December 2022

[156] [redacted] is a cybersecurity technology company which provides endpoint security, threat intelligence and cyberattack response services. - [redacted] (accessed 31 October 2025)

[157] [redacted] is an information security company which offers identity management services focused on privileged access management. - [redacted] (accessed 31 October 2025)

[158] [redacted] is a cloud-based solution that is used to detect vulnerabilities on networked assets, such as servers, network devices (e.g. routers, switches and firewalls), peripherals (e.g. IP-based printers or fax machines) and workstations. - [redacted] (accessed 31 October 2025)

[159] [redacted] is a tool used to discover, classify and validate and analyse credentials machines use to authenticate themselves to one another, such as API keys, database passwords and private encryption keys. - [redacted] (accessed 31 October 2025)

[160] Embedded secrets or embedded credentials are plain text passwords or other secrets (e.g. tokens) within source code. Whilst this can assist setup of digital systems at scale, it poses a significant cybersecurity risk. - What are Hardcoded Passwords/Embedded Credentials? Our... | BeyondTrust (accessed 31 October 2025)

[redacted]

[redacted][161] and [redacted],[162] to monitor and identify potential threats to LastPass and its customers;

g) engaging [redacted][163] to proactively identify and facilitate the takedown of phishing sites that could be used in phishing campaigns against LastPass customers; and

h) additional employee training programs, including company-wide security and privacy awareness training.[164]

156. Following the Incidents, LastPass implemented a revised Acceptable Use Policy[165] which explicitly states that:

a) LastPass employees are provided with a company-owned laptop or desktop computer and a company-owned mobile phone to perform their job function;[166]

b) LastPass employees are prohibited from conducting any business activities on personal or non-managed computing platforms;[167]

c) LastPass employees are prohibited from using their personally owned device to access LastPass-owned or controlled resources, unless this occurs through security sanctioned use cases of Virtual Desktop Interfaces;[168] and

d) where an exception is granted for the use of personally owned

[161] [redacted] is a provider of threat detection and intelligence services. - [redacted] (accessed 31 October 2025)
[162] [redacted] is a tool used by cybersecurity teams to proactively track threats and implement mitigations. - [redacted] (accessed 31 October 2025)
[163] [redacted] (or [redacted]) is a cybersecurity company which specialises in the detection, analysis and mitigation of phishing attacks. - [redacted] (accessed 31 October 2025)
[164] Letter from Paul Hastings(Europe) LLP to the ICO, 15 August 2025
[165] LastPass End User Computing Acceptable Use Policy, Version 2.0 (24 January 2025 and updated 18 February 2025)
[166] LastPass End User Computing Acceptable Use Policy, Version 2.0 (24 January 2025 and updated 18 February 2025), Section 7.3.1
[167] LastPass End User Computing Acceptable Use Policy, Version 2.0 (24 January 2025 and updated 18 February 2025), Section 7.3.2
[168] LastPass End User Computing Acceptable Use Policy, Version 2.0 (24 January 2025 and updated 18 February 2025) Section 7.3.3

[redacted]

mobile phones, LastPass employees are required to comply with additional security requirements, must report any confirmed or suspected security incidents, without delay, to the LastPass Help Centre and must restrict their usage to the mobile Microsoft Authenticator App and not install any other LastPass applications or store any LastPass data even if they have the privileged to do so.[169]

157. In addition, LastPass now requires employees who are working remotely to comply with IT guidelines which contain specific instructions on keeping personal activities and work separate.[170]

158. LastPass informed the Commissioner that, since its operational separation from the GoTo Business in December 2021, it has continued to establish its own independent information security team, including a dedicated incident response function, which has developed a LastPass-specific Incident Management Policy. LastPass also established a Governance Risk and Compliance team which developed a LastPass-specific Security Incident Response Plan, which replaced the revised GoTo's incident response plan initially used on an interim basis after the separation of the GoTo and LastPass Businesses in December 2021.[171]

159. Following the confusion which resulted from the misconfiguration of the email distribution list used by the SOC in the wake of Incident 2, LastPass revised the distribution list to include the company's broader security operations team.[172]

160. The Commissioner considers that the measures taken by LastPass following the Incidents were primarily focused on preventing the occurrence of a similar type of security incident in future and have addressed its previous non-compliance with its obligations under Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR. However, the

[169] LastPass End User Computing Acceptable Use Policy, Version 2.0 (24 January 2025 and updated 18 February 2025), Section 8.1
[170] Letter from Paul Hastings (Europe) Ltd to the ICO, 22 February 2023
[171] Letter from Paul Hastings (Europe) LLP to the ICO, 13 December 2023
[172] Letter from Paul Hastings (Europe) LLP to the ICO, 25 May 2023

[redacted]

Commissioner has found that such measures should be treated as neutral rather than a mitigating factor, as LastPass' actions did not exceed what may reasonably be expected of a controller in these circumstances and, whilst effective in ensuring that LastPass has remediated the infringements of Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR identified in this Notice, had only a limited effect in mitigating the damage and distress suffered by data subjects as a direct result of the Incidents.[173]

(b) The degree of responsibility of the controller or processor (Article 83(2)(d) UK GDPR)

161. At paragraph 81, the *Fining Guidance* refers to the level of accountability expected of controllers and processors under the UK GDPR and indicates that it is more likely that the degree of responsibility will be considered an aggravating, or, at most, a neutral factor.[174]

162. Pursuant to Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR, LastPass was directly responsible for implementing appropriate technical and organisational measures to ensure a level of security of its customers' personal data which was appropriate in light of the sensitivity of the personal data it processed and the nature, purpose and context of its processing operations.

163. When assessing the appropriateness of such technical and organisational measures, the Commissioner considers that it is necessary to have regard, in particular, to:

a) the highly confidential nature of some of the personal data processed by LastPass, including credentials for its customers' online accounts;

b) the nature and purposes of LastPass' processing, specifically the provision of services designed to enhance its customers' online

[173] Fining Guidance, paragraph 76
[174] Relevant aggravating or mitigating factors | ICO

[redacted]

security;

c) the reasonable expectations of LastPass customers regarding the measures in place to protect the personal data they shared with the company; and

d) the increase in remote working in the wake of the Covid-19 pandemic and the increased security risks this posed for controllers, particularly in respect of LastPass employees' use of personal devices to access their Employee Business accounts.

164. When assessing LastPass' degree of responsibility for the Infringements, the Commissioner has considered the extent to which LastPass did what it could reasonably have been expected to do in respect of implementing appropriate technical and organisational security measures, taking into account its size and resources and the nature and purposes of its processing operations.[175]

165. The Commissioner has had particular regard to the fact that LastPass' business is based upon the offer of services which are designed to enhance individuals' and businesses' online security by ensuring that their own and their employees' credentials for their online accounts are sufficiently robust and securely stored. Therefore, the Commissioner considers that data subjects are likely to have chosen LastPass as a password management provider as a result of a desire to enhance their personal digital security and would have been attracted by the company's advertised position as the industry leader in password management, with millions of customers and the promise of "*best-in-class security features.*"[176]

166. As a result, LastPass customers placed a high degree of trust in the company when choosing its services as a means of securely storing their

[175] Fining Guidance, paragraph 79
[176] #1 Password Manager & Vault App with Single-Sign On & MFA Solutions - LastPass (accessed 13 March 2025)

confidential personal data and were entitled to expect that LastPass would adopt an appropriately stringent and diligent approach to its data security obligations under Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR.

167. However, the Commissioner has also taken into account the highly sophisticated and targeted nature of the attack, which was conducted over the course of two separate incidents only a matter of hours apart, with this temporal proximity having limited LastPass' ability to prevent the personal data breach which occurred during Incident 2 after the threat actor had perpetrated Incident 1. The threat actor also deployed a number of obfuscation methods in an attempt to conceal their activity. In Incident 1, the threat actor tampered with the endpoint detection response agent that was installed on the targeted employee's laptop, carried out anti-forensic activity and used a third-party VPN service to disguise the origin of their activity and impersonate the Software Developer. In Incident 2, the threat actor installed a keylogger on the Senior Development Operations Engineer's device to capture their master password, obtained and used a trusted device cookie to bypass LastPass' MFA system and impersonated the targeted employee's credentials and normal activity, resulting in an AWS GuardDuty alert not being triggered until 15 October 2022.[177] In addition, the fact that the personal data stored within the LastPass customers' vaults was only exfiltrated in an encrypted form was directly attributable to the technical security measures implemented by LastPass, specifically its *"zero knowledge"* encryption system.

168. Therefore, the Commissioner finds that, on balance, whilst LastPass bore a high degree of responsibility for complying with its obligations under Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR, the highly sophisticated and targeted nature of the attack and the effectiveness of

[177] LastPass' Written Representations, 9 July 2025: paragraphs 9.7 – 9.12

[redacted]

LastPass' technical and organisational measures in limiting the seriousness of the Incidents, means that LastPass' degree of responsibility should be treated as a neutral rather than an aggravating factor.

(c) Any relevant previous infringements of the controller or processor (Article 83(2)(e) UK GDPR)

169. The Commissioner is not aware of any relevant previous infringements of the UK GDPR or DPA 2018 committed by LastPass. Therefore, this factor is not relevant to the Commissioner's decision.

(b) The degree of cooperation with the Commissioner (Article 83(2)(f) UK GDPR)

170. Pursuant to Article 31 UK GDPR and paragraph 87 of the *Fining Guidance*,[178] controllers and processors are required to cooperate with the Commissioner, on request, in the performance of his tasks. The Commissioner's tasks include the monitoring and enforcement of the UK GDPR[179] and the conduct of investigations into the application of the UK GDPR.[180] Paragraph 87 of the *Fining Guidance* further states that such cooperation on the part of controllers and processors may include, for example, responding to requests for information and attending meetings and that the Commissioner considers that, as this duty of cooperation is required by law, meeting this standard should not be regarded as a mitigating factor.[181]

171. Paragraph 88 of the *Fining Guidance* states that "*the Commissioner may consider it appropriate to view cooperation as a mitigating factor where the controller or processor has responded to requests during the investigation in a way that:*

a) enables the enforcement process to be concluded significantly more

[178] Relevant aggravating or mitigating factors | ICO
[179] Article 57(1)(a) UK GDPR and s.115(2)(a) DPA 2018
[180] Article 57(1)(h) UK GDPR and s.115(2)(a) DPA 2018
[181] Paragraph 87 of the Fining Guidance

[redacted]

quickly or effectively; or

b) significantly limits the harmful consequences for people's rights and freedoms that might otherwise have occurred."

172. LastPass responded to several informal requests for information during the Commissioner's investigation and provided financial information relating to its parent company, LMI Parent, L.P. in response to an Information Notice issued by the Commissioner on 19 September 2024 and a further request from the ICO on 6 August 2025.[182] In doing so, the Commissioner's view is that LastPass demonstrated a good level of cooperation.

173. However, the Commissioner considers that LastPass' level of cooperation during his investigation does not go beyond what is reasonably to be expected of any controller in such circumstances. LastPass submitted that the Commissioner's extensive reliance on the information provided by LastPass to the ICO in the NOI was evidence that its level of cooperation should be treated as a mitigating factor.[183] However, the Commissioner considers that it is inevitable that any notice will extensively rely on the information provided by the controller, which the controller is, in any event, under an obligation to provide following a personal data breach and in the course of an investigation by the ICO pursuant to Article 33 UK GDPR and Article 31 UK GDPR respectively.

174. Therefore, the Commissioner finds that LastPass' degree of cooperation should be treated as a neutral, rather than a mitigating factor.

(c) <u>The manner in which the Infringements became known to the Commissioner (Article 83(2)(h) UK GDPR)</u>

175. Paragraph 90 of the *Fining Guidance* states that "*the Commissioner will have regard to the manner in which the infringement became known to*

[182] Email from the ICO to Paul Hastings (Europe) LLP, 6 August 2025
[183] LastPass' Written Representations, 9 July 2025: paragraph 10.27

[redacted]

the Commissioner, in particular whether, and if so to what extent, the controller or processor notified the Commissioner of the infringement." Whilst the Commissioner may view the controller or processor bringing an infringement to his attention of its own volition as a mitigating factor, this will not be the case if the controller or processor is subject to a statutory duty to comply with notification obligations under the UK GDPR. The Commissioner will not consider a notification required by law, even if made promptly, to be a mitigating factor.[184]

176. Article 33(1) UK GDPR requires a controller to notify the Commissioner of a personal data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

177. LastPass notified the Commissioner of the Incidents on 30 November 2022, over two months after Incident 1 occurred, but within the statutory time limit of 72 hours of it becoming aware of the personal data breach. LastPass became aware that a threat actor had infiltrated its network on 11 August 2022 (in respect of Incident 1) and 15 October 2022 (in respect of Incident 2). LastPass commenced an internal investigation and on 27 November 2022 its investigation team concluded that there was at least a possibility that personal data may have been unlawfully accessed and/or exfiltrated by the threat actor.[185]

178. Therefore, the Commissioner considers that LastPass complied with its obligation under Article 33(1) UK GDPR and consequently, this should be treated as a neutral, rather than an aggravating or mitigating factor.

(d) <u>Measures previously ordered against the controller or processor (Article 83(2)(i) UK GDPR)</u>

179. The Commissioner has not previously imposed measures referred to in

[184] Fining Guidance, paragraphs 91 - 92
[185] LastPass' Initial Personal Data Breach Report (30 November 2022)

[redacted]

Article 58(2) UK GDPR on LastPass. Therefore, this factor is not relevant to the Commissioner's conclusions.

(e) Adherence to approved codes of conduct or certification mechanisms (Article 83(2)(j) UK GDPR)

180. There are no relevant codes of conduct or approved certification mechanisms in this case. Therefore, this factor is not relevant to the Commissioner's conclusions.

(f) Any other applicable aggravating or mitigating factors (Article 83(2)(k) UK GDPR)

181. The Commissioner has concluded that there is no evidence to suggest that LastPass obtained any financial benefit as a result of its failure to implement appropriate technical and organisational measures to ensure the integrity and confidentiality of its processing operations.[186]

182. The Commissioner does not consider that there are any other aggravating or mitigating factors in this case.

Article 83(1) UK GDPR: Effectiveness, Proportionality and Dissuasiveness

183. The Commissioner finds that the imposition of a penalty would, in the circumstances of this case, be an effective, proportionate and dissuasive regulatory response to the Infringements.

184. Taking into account:

a) the seriousness of the Infringements;

b) the number of data subjects affected;

c) the degree of negligence demonstrated by LastPass;

d) the nature of the processing LastPass performs; and

e) the potential consequences of a personal data breach affecting its

[186] Fining Guidance, paragraph 99

[redacted]

processing systems;

the Commissioner has found that the imposition of a penalty would be a proportionate regulatory response. The imposition of a penalty would not exceed what may be considered appropriate and necessary in the circumstances to ensure compliance with UK data protection legislation and to provide an appropriate sanction for the Infringements.

185. LastPass continues to process its customers' personal data. Therefore, the Commissioner considers that there is a need to deter LastPass from committing any further infringements of its security obligations under the UK GDPR in future. The Commissioner also considers that there is a need to deter other controllers and processors operating within the sector from committing similar infringements of Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR. The Commissioner finds that issuing a penalty notice to LastPass in respect of the Infringements would discharge this requirement for both a specific and general deterrent effect.

186. Furthermore, the Commissioner considers that the penalty will raise awareness of the need for controllers and processors, both within the cybersecurity sector and more generally, to ensure that they implement appropriate technical and organisational security measures which take into account the nature, scope, context and purposes of their processing operations, as well as the risks they pose to the interests and fundamental rights and freedoms of data subjects.

187. In reaching his decision to impose a penalty, the Commissioner has also had regard to the desirability of promoting economic growth, as required by section 108 of the Deregulation Act 2015, and the desirability of promoting innovation and competition as required by section 120(a) and (b) DPA 2018 respectively. However, the Commissioner is mindful that the desirability of promoting economic growth, innovation and competition does not legitimise non-compliance with data protection

law. Furthermore, non-compliant activity or behaviour harms the interests of legitimate businesses that are working to comply with data protection law, which disrupts competition and acts as a disincentive to investment in compliance.[187]

C. The Commissioner's conclusions on whether to impose a penalty

188. For the reasons set out above, the Commissioner has decided to impose a monetary penalty on LastPass in respect of the Infringements.

VI. CALCULATION OF THE PENALTY

189. The process the Commissioner follows in deciding the appropriate amount of any penalty which may be imposed in an individual case is described in the *Fining Guidance*,[188] which sets out a five-step penalty setting mechanism:

a) Step 1: An assessment of the seriousness of the infringement in order to determine an appropriate starting point for the penalty.

b) Step 2: Accounting for the turnover of the undertaking when assessing the starting point for the penalty.

c) Step 3: Calculating the starting point for the penalty based on the outcomes of Steps 1 and 2.

d) Step 4: Adjusting the starting point for the penalty on the basis of any relevant aggravating or mitigating factors.

e) Step 5: Adjusting the penalty to ensure that it is effective, proportionate and dissuasive, whilst not exceeding the relevant statutory maximum.

190. In carrying out the assessment, the Commissioner will be mindful that the aim of Steps 1 to 4 set out above is to identify a penalty amount

[187] Fining Guidance, paragraph 105
[188] Fining Guidance, paragraph 106

[redacted]

that is effective, proportionate and dissuasive. The purpose of Step 5 is to provide the opportunity for the Commissioner to check that is the case. Whilst the Commissioner has applied this approach, the overall assessment of the appropriate level of the penalty which the Commissioner intends to impose is not a mechanistic exercise and involves evaluation and judgment, taking into account all the relevant circumstances of the case.[189]

Statutory Maximum Penalty

191. The Commissioner has found that LastPass infringed Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR.

192. An infringement of Article 5(1)(f) UK GDPR is subject to the higher maximum statutory penalty of £17.5 million, or, in the case of an undertaking, 4% of the worldwide turnover in the preceding financial year, whichever is higher.[190]

193. An infringement of Article 32(1) UK GDPR is subject to the standard maximum statutory penalty of £8.7 million, or, in the case of an undertaking, 2% of the worldwide annual turnover in the preceding financial year, whichever is higher.[191]

194. Pursuant to Article 83(3) UK GDPR, if a controller or processor intentionally or negligently, in the course of the same or linked processing operations, infringes several provisions of the UK GDPR, the total amount of any penalty imposed cannot exceed the amount specified for the gravest infringement.[192] Therefore, the Commissioner has based his assessment of the level of the penalty on the higher maximum statutory amount of £17.5 million, or, in the case of an undertaking, 4% of the worldwide turnover in the preceding financial year.

[189] Fining Guidance, paragraphs 142 - 143
[190] Article 83(5)(a) UK GDPR and Section 157(1)(a) DPA 2018
[191] Article 83(4)(a) UK GDPR and Section 157(1)(a) DPA 2018
[192] Also see paragraph 33 of the Fining Guidance

[redacted]

195. The *Fining Guidance* considers the concept of an undertaking for the purpose of imposing a penalty at paragraphs 23 – 31. Where a controller or processor forms part of an undertaking, the Commissioner will calculate the maximum penalty based on the turnover of the undertaking as a whole. Whether or not a controller or processor forms part of an undertaking depends on whether another legal or natural person, for example, a parent company, exercises decisive influence over it.

196. Paragraphs 28 to 30 of the *Fining Guidance*[193] state:

> "*In this context, an undertaking does not correspond to the commonly understood notion of a legal entity or a company under, for example, English commercial or tax law. Instead, an undertaking may comprise one or more legal or natural persons forming a 'single economic unit', rather than a single entity characterised as having legal personality.*
>
> *Whether or not an individual controller or processor forms part of a wider undertaking depends on whether it can act autonomously or whether another legal or natural person, for example, a parent company, exercises decisive influence over it.*
>
> *Where a parent company owns all, or nearly all, the voting shares in a subsidiary, there is a presumption that the parent company exercises decisive influence over the subsidiary's conduct. This presumption may be rebutted. However, the burden is on the parent company to provide sufficient evidence to demonstrate that the subsidiary acts independently."*[194]

[193] The concept of an 'undertaking' for the purpose of imposing fines | ICO

[194] The approach set out in the Fining Guidance is consistent with the decision of the CJEU in *ILVA A/S* [C-383/23] (13 February 2025), in which the Court held that, when assessing the amount of the administrative fine to be issued to a subsidiary within the Lars Larsen Group, the group in its entirety was the relevant undertaking and the maximum statutory fine had to be calculated on the basis of the group's total worldwide annual turnover in the preceding financial year. Whilst the decisions of the CJEU are no longer binding as a matter of UK law following the UK's departure from the European Union, pursuant to section 6(2)

[redacted]

197. The relevant controller responsible for the Infringements in respect of UK data subjects is LastPass. LastPass is a wholly-owned subsidiary of LastPass Ireland Limited, with both companies forming part of the corporate group ultimately headed by LMI Parent, L.P, which operates both the LastPass and GoTo Businesses, albeit as distinct commercial operations. In the NOI, the Commissioner relied upon the presumption referred to in paragraph 196 above, that the parent company, LMI Parent, L.P., exercises decisive influence over its indirectly wholly-owned subsidiary LastPass and therefore calculated the maximum provisional penalty on the basis of the turnover of LMI Parent L.P.

198. In its Written Representations and at the Oral Hearing, LastPass challenged the Commissioner's reliance upon the rebuttable presumption that LMI Parent, L.P. exercises decisive influence and control over its indirectly wholly-owned subsidiary LastPass and submitted that any penalty to be imposed should be calculated on the basis of the turnover of the LastPass Business.[195]

199. Recital 150 of the UK GDPR states that "*Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102* [of the Treaty of the Functioning of the European Union ("**TFEU**")]." Articles 101 and 102 TFEU relate to competition within the European Union's internal market. Therefore, the rebuttable presumption in paragraph 30 of the *Fining Guidance* has been derived from European Union competition case law, including the case of *Akzo Novel NV & Ors v European Commission [2009] [ECLI:EU:C:2009:536] [C-97/08]* where, at paragraphs 60 and 61, the Court of Justice of the European Union stated that "*In the specific case where a parent company has a 100% shareholding in a subsidiary which has infringed the Community*

of the European Union (Withdrawal) Act 2018, UK courts and tribunals may have regard to decisions of the CJEU issued after 31 December 2020 in so far as they are relevant to any matter before them.

[195] LastPass' Written Representations, 9 July 2025: paragraph 11.8

[redacted]

competition rules, first, the parent company can exercise a decisive influence over the conduct of the subsidiary… and, second, there is a rebuttable presumption that the parent company does in fact exercise a decisive influence over the conduct of its subsidiary… In those circumstances, it is sufficient for the Commission to prove that the subsidiary is wholly owned by the parent company in order to presume that the parent exercises a decisive influence over the commercial policy of the subsidiary. The Commission will be able to regard the parent company as jointly and severally liable for the payment of the fine imposed on its subsidiary, unless the parent company, which has the burden of rebutting that presumption, adduces sufficient evidence to show that its subsidiary acts independently on the market."

200. After taking into account the representations made by LastPass, the Commissioner has concluded that LastPass has not produced objective evidence which is sufficient to rebut the presumption that LMI Parent, L.P. exercises decisive influence and control over the LastPass Business by virtue of its indirect 100% share ownership of the subsidiaries, which collectively constitute the LastPass Business, including LastPass. Therefore, the Commissioner has concluded that the relevant undertaking for the purpose of calculating the statutory maximum penalty in this case is LMI Parent, L.P.

201. On 22 August 2025, LastPass provided consolidated financial statements for LMI Parent, L.P. and its subsidiaries for the year ending 31 December 2024.[196] The consolidated financial statements showed that, for the year ending 31 December 2024, LMI Parent, L.P. recorded a turnover of [redacted] (approximately £[redacted]).[197] 4% of this figure is £[redacted]. As this is greater than the higher maximum statutory

[196] Email from Paul Hastings (Europe) LLP to the ICO, 22 August 2025

[197] For the purposes of this calculation, the Commissioner has used the average of the Pound sterling and US Dollar exchange rates on the first and last trading days of the period covered by LMI Parent, L.P.'s consolidated financial statements (2 January 2024 and 31 December 2023)

[redacted]

penalty of £17.5 million set out in Article 83(5)(a) UK GDPR, the calculation of the penalty will proceed based on a statutory maximum of £[redacted].

A. Step 1: Assessment of the seriousness of the Infringements

202. As set out in paragraphs 109 to 115 of the *Fining Guidance*, the Commissioner determines a starting point for the penalty by first assessing the seriousness of the infringement. The Commissioner categorises the infringement according to its degree of seriousness and then selects a starting point based on a percentage of the relevant applicable statutory maximum.

203. As stated at paragraph 147 above, the Commissioner has categorised the Infringements as having a low degree of seriousness. This means that the starting point will be between 0% and 10% of the relevant legal maximum.

204. The Commissioner finds that the Infringements warrant a starting point of 5% of the applicable legal maximum. A starting point lower than 5% is not warranted due to the extent of LastPass' failure to implement appropriate technical and organisational security measures during the Relevant Period. The Commissioner's full assessment of the seriousness of the Infringements is set out at paragraphs 109 to 147 above.

205. In determining that a starting point higher than 5% is not warranted in the circumstances of this case, the Commissioner has taken into account the fact that the Infringements were not committed intentionally, the limited evidence of realised material damage to affected data subjects, the fact that the personal data stored within customer vaults remained encrypted even when exfiltrated by the threat actor due to LastPass' "*zero-knowledge*" encryption system and the steps LastPass took in response to the Incidents in an attempt to mitigate their impact and bring its processing operations into compliance with Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR.

[redacted]

B. Step 2: Accounting for turnover

206. Having assessed the seriousness of the infringement, the Commissioner next determines whether any adjustments are necessary to account for turnover, as set out in paragraphs 116 to 129 of the *Fining Guidance*. This step permits the Commissioner to adjust the starting point to reflect the size of the undertaking. This approach aids the Commissioner in ensuring that the penalty figure is effective, proportionate and dissuasive.

207. As referred to in paragraph 183 above, LMI Parent, L.P.'s turnover for the year ending 31 December 2024 was $[redacted] (approximately £[redacted]). This means that no adjustment has been made to the starting point. In cases such as this, where the higher statutory maximum in Article 83(5)(a) UK GDPR applies and the global turnover of the undertaking in the previous financial year is greater than £437.5 million, the undertaking's size is already deemed to be reflected by the use of a percentage figure to calculate the statutory maximum and the Commissioner will consider whether it is appropriate to impose a penalty up to the amount allowed by law.[198]

C. Step 3: Calculation of the starting point

208. The starting point for the penalty in this case has been calculated as follows:

Turnover ([redacted]) x statutory maximum amount (4%) x adjustment for seriousness (5%) = **£**[redacted]

D. Step 4: Adjustment to take into account any aggravating or mitigating factors

209. The Commissioner next takes into account any aggravating or mitigating factors. These factors may warrant an increase or decrease in the

[198] Fining Guidance: Table B: Ranges for adjustment based on the turnover of the undertaking

[redacted]

penalty calculated at the end of Step 3 (the starting point of £[redacted]).

210. The examination of whether there are any aggravating or mitigating factors present in this case is set out in full at paragraphs 148 – 182 above. In summary:

a) LastPass took steps to mitigate the impact of the Incidents once it became aware of the unauthorised access to and exfiltration of personal data from the Backup Database, and has implemented a range of measures to bring its processing activities into compliance with Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR. However, the Commissioner has found that the measures taken by LastPass in response to the Incidents were primarily focused on remedying the Infringements, had only a limited effect on mitigating the direct impact of the Incidents on data subjects and did not go beyond what may reasonably be expected of a controller in the circumstances. Therefore, the Commissioner has found that LastPass' attempts to mitigate the damage suffered as a result of the Infringements should be treated as a neutral factor (see paragraphs 148 – 160 above).

b) LastPass is wholly responsible for the Alleged Infringements. The Commissioner has found that due to the nature of its business, the confidentiality of the personal data it processes and the reasonable expectations of its customers, LastPass was subject to a high level of responsibility for compliance with its security obligations under Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR. However, in light of the sophisticated and highly targeted nature of the attack and the effectiveness of LastPass' technical and organisational measures in limiting the personal data that the threat actor was able to access and exfiltrate in an unencrypted form, the Commissioner has concluded that LastPass' level of responsibility does not warrant an increase in the amount of the penalty (see

[redacted]

paragraphs 161 – 168 above).

c) The Commissioner is not aware of any previous infringements of the UK GDPR by LastPass; nor has he previously imposed any measures referred to in Article 58(2) UK GDPR on LastPass. Therefore, these factors are not relevant to the Commissioner's decision to impose a penalty (see paragraphs 169 and 179 above).

d) LastPass has cooperated with the Commissioner to the extent required by Article 31 UK GDPR, which, in accordance with paragraph 87 of the *Fining Guidance*, has been treated as a neutral factor (see paragraphs 170 – 174 above).

e) There are no relevant codes of conduct or approved certification mechanisms in this case. Therefore, this factor is not relevant to the Commissioner's decision to impose a penalty (see paragraph 180 above).

f) There are no other relevant aggravating or mitigating factors in this case (see paragraphs 181 and 182 above).

211. In light of the above, the Commissioner has concluded that no adjustment should be made to take account of aggravating or mitigating factors.

E. Step 5: Adjustment to ensure the penalty is effective, proportionate and dissuasive

212. As set out in paragraph 142 of the *Fining Guidance*,

"*The aim of Steps 1 to 4 of the calculation is to identify a fine that is effective, proportionate and dissuasive. The purpose of Step 5 is to provide the opportunity to check that is the case. It allows the Commissioner to increase or decrease the penalty as necessary, having regard to all the relevant circumstances of each individual case.*"

213. When reaching a decision as to whether a penalty is effective, proportionate and dissuasive, the Commissioner will have regard to all

[redacted]

the relevant circumstances of each individual case. This includes:

a) the seriousness of the infringement;

b) any aggravating or mitigating factors;

c) the controller or processor's size and financial position; and

d) the need for effective deterrence.[199]

214. The *Fining Guidance* also states that the Commissioner will generally take into account an undertaking's total worldwide annual turnover as the primary indicator of its size and financial position. However, the Commissioner will also consider other financial indicators, where relevant, such as profits, net assets and dividends.

215. When assessing whether the penalty calculated after the application of steps 1 to 4 of the *Fining Guidance* would be effective, proportionate and dissuasive, the Commissioner has taken into account the following factors:

a) infringements of Article 5(1)(f) UK GDPR are subject to the higher statutory maximum penalty under Article 83(5)(a) UK GDPR (£17.5 million or, in the case of an undertaking, 4% of the total worldwide annual turnover of the undertaking in the preceding year, whichever is higher);

b) LastPass forms part of a wider undertaking, namely the corporate group led by LMI Parent L.P. which recorded a turnover of $[redacted] (approximately [redacted]), meaning that the statutory maximum in this case is £[redacted];

c) the scope of the Infringements and the Commissioner's investigation, specifically that they only concerned the LastPass Business and not the operations of the GoTo Business, which have operated as separate and distinct business units since the business

[199] Fining Guidance, paragraph 147

[redacted]

restructuring in December 2021;

d) the personal data breach in this case resulted from a highly targeted attack by a sophisticated threat actor who used a variety of methods to obscure their activity and exploited a vulnerability in a piece of third-party software to obtain access to the personal device of the Senior Development Operations Engineer targeted in Incident 2;

e) personal data stored within LastPass customers' vaults remained encrypted at all times due to the protection afforded by LastPass' "*zero knowledge"* encryption system;

f) the Commissioner's investigation did not uncover any evidence of material damage being suffered by data subjects as a result of the Infringements, with realised harm limited to distress resulting from LastPass customers' loss of control over their personal data and the unauthorised access to and exfiltration of such data, as demonstrated by the significant increase in the number of cancellation requests LastPass received in the wake of the Incidents and the complaints submitted by data subjects to both LastPass and the ICO;

g) the absence of evidence indicating that special category data within the meaning of Article 9(1) UK GDPR has, to date, been affected by as a result of the Infringements; and

h) LastPass has now implemented a significant array of measures which have brought its processing systems and services into compliance with Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR. Specifically, LastPass now prevents its employees from linking their Employee Business and Personal accounts, provides all employees with company-issued laptops and mobile phones, as well as [redacted] authorisation keys for enhanced MFA[200] and

[200] Letter from Paul Hastings (Europe) LLP to the ICO, 15 August 2025

[redacted]

prohibits the use of personal devices for corporate activity.

216. In light of the above, the Commissioner considers that a penalty of £[redacted] would represent a disproportionately high penalty in the circumstances of the case, particularly when taking into account the measures that LastPass had in place at the time of the Incidents, the effectiveness of its *"zero knowledge"* encryption system in protecting the personal data stored in LastPass customers' vaults and the steps that LastPass took both in the immediate aftermath of the Incidents and subsequently in order to bring its processing into compliance with the UK GDPR. Therefore, the Commissioner has concluded that a 30% reduction should be applied to ensure that the penalty is effective, proportionate and dissuasive, resulting in a revised penalty of £1,228,283.

217. The Commissioner considers that a penalty of £1,228,283 constitutes an effective, proportionate and dissuasive response to the Infringements. A penalty in this amount would be an appropriate, and not excessive, response to the Infringements and would achieve the objective of promoting LastPass's future compliance with the UK GDPR and DPA 2018.

218. The Commissioner considers that the penalty will have a genuine deterrent effect, as it would be sufficient to deter LastPass specifically, and controllers and processors generally, against future infringements of the UK GDPR and/or DPA 2018.

219. The Commissioner considers that the penalty would also reinforce the importance which the Commissioner attaches to compliance with the security obligations imposed by Article 5(1)(f) UK GDPR and Article 32(1) GDPR and indicate that there are serious consequences for controllers and processors which breach their obligations under these provisions. The Commissioner also finds that the penalty would appropriately reflect the seriousness of personal data breaches affecting

[redacted]

confidential personal data of the type processed by LastPass and the impact on data subjects who entrusted their personal data to LastPass in the expectation that it would be subject to robust safeguards.

220. The Commissioner has balanced these factors against the effectiveness of LastPass' "*zero knowledge"* encryption system, the sophisticated and highly targeted mature of the attack, the absence of any evidenced material harm to data subjects, the lack of any evidence that LastPass intentionally failed to comply with its obligations under the UK GDPR and the measures that LastPass has implemented to improve its technical and organisational security posture in the wake of the Incidents.

221. The Commissioner also considers that the penalty amount is proportionate when taking into account the total revenues of the corporate group led by LMI Parent, L.P. The penalty represents approximately [redacted]% of LMI Parent, L.P.'s turnover during the financial year ending 31 December 2024[201] and approximately 8.5% of the turnover generated by LastPass in the year ending 31 December 2023.[202] The penalty amount is not more than the Commissioner considers to be appropriate and necessary in the circumstances in order to reflect the seriousness of the Infringements, nor does it exceed the applicable statutory maximum.

F. Conclusion - Penalty

222. For the reasons set out above, the Commissioner has decided to impose

[201] In *ILVA A/S* [C-383/23] (13 February 2025) at [29], the CJEU held that only an administrative which takes into account the infringements of the EU GDPR and, where appropriate, the actual or material economic capacity of the person on which the fine is imposed, is capable of satisfying the Article 83(1) EU GDPR requirement for the fine to be effective, proportionate and dissuasive, The Court stated that in order to assess those conditions, it is necessary to take account of whether the person on which the fine is imposed forms part of an undertaking within the meaning of Articles 101 and 102 of the Treaty on the Functioning of the European Union.

[202] LastPass UK Ltd's accounts for the year ending 31 December 2023 are the latest that are available from Companies House. - LASTPASS UK LTD filing history - Find and update company information - GOV.UK

[redacted]

a monetary penalty on LastPass in the amount of **£1,228,283**.

VII. FINANCIAL HARDSHIP

223. The *Fining Guidance* outlines that, in exceptional circumstances, the Commissioner may reduce a penalty where an organisation is unable to pay due to its financial position.

224. The Commissioner received no representations from LastPass in relation to financial hardship.

VIII. PAYMENT OF THE PENALTY

225. The penalty must be paid to the ICO by BACS transfer or cheque by 19 December 2025 or in accordance with any agreed payment plan.

226. Pursuant to paragraph 9(1) of Schedule 16 to the DPA 2018, the Commissioner cannot take action to recover a penalty unless:

a) the period specified in this Penalty Notice (i.e. by 19 December 2025) has ended;

b) any appeals against this Penalty Notice have been decided or otherwise ended;

c) if this Penalty Notice has been varied, any appeals against the penalty variation notice have been decided or otherwise ended; and

d) the period for LastPass to appeal this Penalty Notice, and any variation of it, has ended.

227. Under paragraph 9(2) of Schedule 16 to the DPA 2018, in England and Wales, the Commissioner is able to enforce the payment of the penalty. The penalty is recoverable:

a) if the County Court so orders, as if it were payable under an order of that court; or

b) if the High Court so orders, as if it were payable under an order of that court.

[redacted]

IX. RIGHTS OF APPEAL

228. By virtue of section 162 DPA 2018, LastPass may appeal to the First-tier Tribunal (General Regulatory Chamber) (Information Rights) against this Penalty Notice. LastPass may appeal to the Tribunal against the amount of the penalty regardless of whether or not it appeals against this Penalty Notice.

229. Information about the appeals process is set out in **Annex 1** to this Penalty Notice. Any notice of appeal should be sent or delivered to the Tribunal so that it is received within 28 days of the date of this Penalty Notice.

Dated the 20 November 2025

Signed: [redacted]

Andy Curry
Head of Investigations (Criminal)
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

[redacted]

ANNEX 1

DATA PROTECTION ACT 2018 (PART 6, SECTION 162)

RIGHTS OF APPEAL

1. By virtue of section 162(1) DPA 2018, LastPass may appeal to the Tribunal against this Penalty Notice. By virtue of section 162(3) DPA 2018, LastPass may appeal to the Tribunal against the amount of the penalty specified in this Penalty Notice, regardless of whether or not LastPass appeal against this Penalty Notice.

2. If LastPass appeals and if the Tribunal considers:

   a) that the notice or decision against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice or decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently,

   the Tribunal must allow the appeal or substitute another notice or decision which the Commissioner could have given or made.

3. LastPass may bring an appeal by sending notice of appeal to the Tribunal at:

   grc@justice.gov.uk

   or

   General Regulatory Chamber
   HM Courts and Tribunals Service
   PO Box 11230
   Leicester
   LE1 8FQ
   UK
   (Telephone: 0300 123 4504)

4. The notice of appeal should be received by the Tribunal within 28 days of the date of this Penalty notice (which is the date that this Penalty Notice was sent).

[redacted]

5. If LastPass' notice of appeal is late, the Tribunal will not accept it unless the Tribunal has extended the time for complying with this rule.

6. The notice of appeal **must** include:

   a) LastPass' name and address;

   b) the name and address of LastPass' representative (if any);

   c) an address where documents may be sent or delivered to LastPass;

   d) the name and address of the respondent (the Information Commissioner);

   e) details of the decision to which the proceedings relate;

   f) the result LastPass is seeking;

   g) the grounds on which LastPass relies;

   h) a full copy of this Penalty Notice; and

   i) (if the notice of appeal is late) a request for an extension of time, giving the reason(s) why the notice of appeal is late and why the Tribunal should accept it.

7. Before deciding whether or not to appeal LastPass may wish to consult its solicitor or another adviser. At the hearing of an appeal a party may conduct their case themselves, or may be represented by any person whom they may appoint for that purpose.

8. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the DPA 2018 and The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules (Statutory Instrument 2009 No. 1976 (L.20)).

[redacted]

ANNEX 2
INCIDENT DIAGRAM